IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



| | |
|---|---|
| In Re the Application of | : **Naoki OGUCHI** |
| Filed: | : **Concurrently herewith** |
| For: | : **PACKET RELAYING APPARATUS AND....** |
| Serial No. | : **Concurrently herewith** |

Assistant Commissioner for Patents
Washington, D.C. 20231

March 5, 2002

**PRIORITY CLAIM AND SUBMISSION**

**OF PRIORITY DOCUMENT**

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-062685** filed **March 6, 2001,** a certified copy of which is enclosed.

Respectfully submitted,

Brian S. Myers
Reg. No. 46,947

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: FUJ 19.011
TELEPHONE: (212) 940-8800

# 日　本　国　特　許　庁
## JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　３月　６日

出願番号
Application Number: 特願２００１－０６２６８５

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　８月３１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０８０８８２

【書類名】　特許願
【整理番号】　0052258
【提出日】　平成13年 3月 6日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/56
【発明の名称】　パケット中継装置およびパケット中継方法
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小口　直樹
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100108187
【弁理士】
【氏名又は名称】　横山　淳一
【電話番号】　044-754-3035
【手数料の表示】
【予納台帳番号】　011280
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0017694
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　パケット中継装置およびパケット中継方法

【特許請求の範囲】

【請求項１】　入力されたパケットに対応する送信元仮想閉域網識別子に基づき、該パケットの中継が許されている１つ以上の仮想閉域網を選択する手段と、

前記１つ以上の仮想閉域網に対応する１つ以上の経路ドメインを選択する手段と、

前記パケットの送信先アドレスと前記１つ以上の経路ドメインの各経路ドメイン情報とを照合し、前記パケットを次のパケット中継装置に送出するための送出アドレスを選択する手段と、

前記送出アドレスに前記パケットを送出する手段を有することを特徴とするパケット中継装置。

【請求項２】　入力されたパケットの送信元仮想閉域網識別子に基づき、該パケットの中継が許されている１つ以上の仮想閉域網を選択するステップと、

前記１つ以上の仮想閉域網に対応する１つ以上の経路ドメインを選択するステップと、

前記パケットの送信先アドレスと前記１つ以上の経路ドメインの各経路情報とを照合し、前記パケットの送出先アドレスを選択するステップと、

前記送出先アドレスに前記パケットを送出するステップを有することを特徴とするパケット中継方法。

【請求項３】　複数の送信元仮想閉域網識別子と該各送信元仮想閉域網識別子に対応する１つ以上の宛先仮想閉域網識別子を管理するポリシ管理部と、

前記ポリシ管理部から1つ以上の送信元仮想閉域網識別子と該１つ以上の各送信元仮想閉域網識別子に対応する１つ以上の宛先仮想閉域網識別子を該１つ以上の各送信元仮想閉域網識別子に対応させて端末に表示する表示部と

を備えることを特徴とするパケット中継装置。

【請求項４】　各宛先仮想閉域網識別子と該各宛先仮想閉域網識別子に対応する１つ以上の経路ドメイン識別子を管理する仮想閉域網管理部を備え、

前記仮想閉域網管理部は端末から入力される１つの宛先仮想閉域網識別子と該１つの宛先仮想閉域網識別子に対応する１つ以上の経路ドメイン識別子を対応させて前記端末に表示する表示部と

を備えることを特徴とするパケット中継装置。

【請求項５】　端末からの指示に基づきドメイン間中継ポリシテーブルに設定された各送信先仮想閉域網識別子および前記各送信先仮想閉域網識別子に対応する経路ドメインの一覧を要求する手段と、

前記要求に基づいてドメイン間中継ポリシテーブルから１つ以上の送信先仮想閉域網識別子を抽出し、前記各送信先仮想閉域網識別子に対応する経路ドメインの一覧を抽出する手段と、

抽出された前記各送信先仮想閉域網識別子および前記各送信先仮想閉域網識別子に対応する経路ドメインの一覧を前記端末に表示する手段を備えることを特徴とするパケット中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信サービスを提供するパケット中継装置及びパケット中継方法に関し、特に、仮想閉域網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）間及び経路ドメイン間でのパケットの中継に関するパケット中継装置及びそのパケット中継方法に関する。なお、以下、経路ドメインをドメインと呼ぶことがある。

【０００２】

【従来技術】

近年、インターネットの普及により、ユーザ（例えば、企業や大学など）ではＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ　Ｔｒａｎｓｆｅｒ　Ｍｏｄｅ）やＦＲ（Ｆｒａｍｅ　Ｒｅｌｙ）などによる仮想専用線（Ｖｉｒｔｕａｌ　Ｐａｔｈ／Ｖｉｒｔｕａｌ　Ｃｈａｎｎｅｌ）を利用しなくとも、分散する各拠点間はインターネットを介して通信できるようになった。この通信ではＶＰＮを構築することがある。以降、ＶＰＮを仮想閉域網と呼ぶことがある。

【０００３】

そして、ユーザのネットワーク内に限ってＩＰアドレスを独自に割り当て、運用するユーザが現れてきている。このようなユーザのネットワーク内でプライベートのＩＰアドレスを使用した場合、そのプライベートＩＰアドレスを有するパケットをそのままグローバルのＩＰアドレスを持つインターネットに流すことはできない。

【０００４】

プライベートのＩＰアドレスとグローバルのＩＰアドレスがインターネット上で重複して使用されることになり、インターネットを介した通信を正常に行うことができない可能性が生じるためである。

【０００５】

したがって、このようなユーザのプライベートネットワークの各拠点間でインターネットを経由して通信を行うときには、このユーザ内のプライベートネットワークからインターネットへの接続では、例えば、グローバルＩＰアドレスを持つＩＰパケットでカプセル化（トンネリング化）してインターネットに転送し、受信側拠点のインターネット網接続ルータでカプセル化されたこのパケットを受信すると同時にカプセル化を解き、受信側の拠点内の宛先ホストにルーティングするといった仕組みが必要となる。

【０００６】

この場合、ユーザは、プライベートのＩＰアドレスを有するＩＰパケットをグローバルＩＰアドレスによりトンネル（送信側ではカプセル化、受信側ではデカプセル化）する装置を備える必要がある。すなわち新たな機器の導入が生じる。

【０００７】

また、カプセル化、デカプセル化する処理が新たに必要となるため性能が低下する可能性もある。なお、以下の記述において中継装置をルータと記述することがある。

【０００８】

さらに、ユーザにおいて、各拠点をそれぞれインターネットに接続する際、各拠点のルータにおいて、経路制御および論理インタフェース等の設定は、各拠点

間の設定の組み合わせ数が増加するにつれてより複雑になる。この場合、ネットワーク機器の導入・維持管理およびネットワーク管理者の育成にコストがかかるという問題がある。

【０００９】

そこで、ユーザがインターネットを介して各拠点間を通信するＶＰＮを導入する場合、そのＶＰＮの導入・維持管理をプロバイダ（本発明ではキャリアを含む）にアウトソース（委託）することにより、ユーザは既存のネットワークにほとんど手を加えることなしにＶＰＮサービスの提供を受けることができる。

【００１０】

このＶＰＮサービスでは、トンネルの始終端機能をプロバイダのルータで実現する。そして、あるユーザが複数の拠点を持っている場合、プロバイダのルータは送信元のユーザ拠点から受信したＩＰパケットをどの宛先ユーザ拠点のネットワークにカプセル化して送信すべきか決定する経路制御機能を備えている。

【００１１】

この機能は、アウトソースによりプロバイダのルータが提供する。このようにプロバイダによりＶＰＮサービスが行われ場合、プロバイダのエッジルータでは、インターネット網の経路制御機能とは別にユーザネットワーク固有の経路制御機能によりＩＰパケットが転送される。

【００１２】

したがって、プロバイダが提供するＶＰＮサービスは、各ユーザの各拠点ネットワークごとに経路制御機能を独立に管理する必要性があることからその設定が非常に複雑になる。

【００１３】

ユーザがＶＰＮを構築することもあるが、ここではプロバイダがＶＰＮを構築しユーザにＶＰＮサービスを提供することを前提に説明する。ネットワークを管理する主体の観点から分類すると、複数拠点の管理主体が同一であるネットワークを「イントラネット（Ｉｎｔｒａｎｅｔ）」と呼び、例えば、管理主体が同一企業により運用されるネットワークを示す。

【００１４】

また複数拠点の管理主体が同一でないネットワークを「エクストラネット（Ｅｘｔｒａｎｅｔ）」と呼び、例えば、異なる独立した企業により運用されるネットワークを示す。また、イントラネットおよびエクストラネットのそれぞれがどのような経路ドメインから構成されているかといった観点からも分類することができる。

【００１５】

すなわち、１つのネットワークが単一の経路ドメインから構成されている場合をシングルドメインと呼び、複数の経路ドメインから構成されている場合をマルチドメインと呼ぶ。このように、シングルドメイン／マルチドメイン，イントラネット／エクストラネットの組み合わせによるネットワーク構成の例を図１に示す。なお、全図をとおして同じ参照符号は同一物または同等物を示す。

【００１６】

しかしながら、一般的にはイントラネットにおいて一つの管理主体が管理するネットワーク内で複数の経路ドメインが存在することは少ないので、本明細書では、以下単にイントラネットといった場合は、シングルドメインのイントラネットを示すものとする。

【００１７】

また、エクストラネットにおいては、複数の管理主体が管理するそれぞれのネットワークで異なる中継ルール（ポリシ）を持っていることが多いと考えられるため、以下単にエクストラネットと呼ぶ場合は、マルチドメインのエクストラネットを示すものとする。

【００１８】

次に、図２および図３は、前述の図１に示すシングルドメイン、マルチドメイン構成のＶＰＮを収容するルータがどのように中継テーブルを構成するかを説明している。

－　第１の従来技術

図２はプロバイダを介して接続されるシングルドメイン構成のイントラネットＶＰＮを収容するルータの中継テーブルの構成例を説明する図である。

【００１９】

図中、パケット受信部１１３はドメイン識別テーブル１０９を参照し、入力されたパケットの送信元経路ドメインを識別する。そして、そのパケットがルーティングパケットである場合は、イントラネットドメイン経路情報処理部１０１に送出される。

【００２０】

例えば、図示していない経路ドメイン＃１１からのルーティングパケットである場合には、イントラネットドメイン経路情報管理部１０２（図中、左側）では、そのルーティングパケットを受信し、各ＶＰＮに対応して設けられたＶＰＮ＃１１に対応するイントラネットドメイン中継テーブル１０４（図中、左側）に書き込む。すなわち、経路ドメイン＃１１からのパケットは経路ドメイン＃１１のみに中継することができる。

【００２１】

一方、図示していない経路ドメイン＃１２に対応するイントラネットドメイン経路情報管理部１０２（図中、右側）はＶＰＮ＃１１及びＶＰＮ＃１２のイントラネットドメイン中継テーブル１０４（図中，左及び右側）に書き込みを行う。すなわち、経路ドメイン＃１２からのパケットは、経路ドメイン＃１１及び経路ドメイン＃１２の両方に中継することができる。このように経路ドメイン＃１１及び経路ドメイン＃１２との間の接続性可否の処理をイントラネットドメイン経路情報管理部１０２と対応するイントラネットドメイン中継テーブル１０４との連携により処理していた。

【００２２】

パケット中継部１１１はパケット受信部１１３からパケットを受信した場合には、送信先ＩＰアドレスに基づき各ＶＰＮに対応する各イントラネットドメイン中継テーブル１０４を順次検索し、該パケットを転送すべき次ホップルータのＩＰアドレスを求める。

【００２３】

そして、パケット送信部１１２の出力インタフェース情報とともに送信先の該ＩＰアドレスを有するパケットをパケット送信部１１２に送出する。パケット送信部１１２は指示された出力インタフェースを選択し、該パケットを送出する。

なお、送信先ＩＰアドレスが各ＶＰＮに対応するイントラネットドメイン中継テーブル１０４に存在しなかった場合、そのパケットは破棄される。

【００２４】

各イントラネットドメイン中継テーブル１０４は、送信先ＩＰアドレス，ＩＰアドレスマスク情報、出力インターフェイス情報、次ホップルータＩＰアドレス等を含むように構成する。

【００２５】

また、定期的に、イントラネットドメイン経路情報処理部１０１が保有する経路ドメイン情報をルーティングパケットに含めてパケット送信部１１２に送出し、パケット送信部１１２は該ルーティングパケットを隣接のルータに配布する。

－　第２の従来技術

図３はマルチドメイン構成のエクストラネットＶＰＮを収容するルータの中継テーブルの構成例を説明する図である。図２と図３との本質的な相違点は、イントラネットからエクストラネットに対応できるように変更されていること、およびドメイン定義部１０５Ａとエクストラネット間中継ポリシ１０７Ａを新たに設けた点である。この相違点に着目し、説明する。

【００２６】

図中、エクストラネットドメイン経路情報処理部１０１Ａのエクストラネットドメイン経路情報管理部１０２Ａは、通常、ルータが管理している経路ドメインの数だけ存在する。送信元の経路ドメインに対応するエクストラネットドメイン経路情報管理部１０２Ａはルーティングパケットを受信し、そのパケットの送信元の経路ドメインに対応するエクストラネットドメイン中継テーブル１０４Ａにルーティング情報を書き込む。

【００２７】

パケット中継部１１１はパケット受信部１１３からパケットを受信した場合には、そのパケットの送信元の経路ドメイン情報に対応するエクストラネットドメイン中継ポリシ１０７Ａを検索し、該パケットを中継できる経路ドメインの一覧を検索する。そして、取得した経路ドメインの一覧および送信先ＩＰアドレスをパラメタにしてドメイン定義部１０５Ａを呼び出す。

【００２８】

ドメイン定義部１０５Ａはパラメタとして与えられた経路ドメインの一覧から順次経路ドメインを取り出し、送信先ＩＰアドレスを用いて該経路ドメインに対応するエクストラネットドメイン中継テーブル１０４Ａを検索し、該パケットを転送すべき次ホップルータのＩＰアドレスを求める。

【００２９】

そして、パケット送信部１１２の出力インタフェース情報とともに送信先の該ＩＰアドレスを有するパケットをパケット送信部１１２に送出する。パケット送信部１１２は指示された出力インタフェースを選択し、該パケットを送出する。

【００３０】

このようにパケットの中継処理では、ある送信元のイントラネットＶＰＮやエクストラネットＶＰＮから送信先ＶＰＮとなる他のエクストラネットやマルチドメインで構成されるイントラネットへの中継ポリシを定義したい場合、次の課題がある。

【００３１】

【発明が解決しようとする課題】

第１の従来技術に示した構成では、各送信元経路ドメインに対する各ＶＰＮ中継テーブルに送信先ＶＰＮに対応する経路情報を書き込む。このため、同じ送信先ＶＰＮに対し複数の送信元ＶＰＮが接続性を定義しようとした場合、複数の送信元ＶＰＮに対する中継テーブルに同じ送信先ＶＰＮの経路情報がコピーされ、全体としてメモリを多く消費する。

【００３２】

第２の従来技術に示した構成では、送信元ＶＰＮを構成するドメインと、送信先ＶＰＮの複数のドメイン間との全ての組み合わせに対し中継ポリシを個別に定義する必要があり、中継ポリシの設定／変更が複雑である。

【００３３】

以上から本発明の第１の課題は、中継ポリシの設定／変更を容易にすることであり、また、本発明の第２の課題は、中継装置で使用されるメモリの使用量の削減することとし、第1及び第2の課題のうち、少なくとも１つの課題を解決するこ

とを目的とする。

【００３４】

【課題を解決するための手段】

本発明は、上述した課題を解決するために以下の構成をとる。

本発明のパケット中継装置は、入力されたパケットに対応する送信元仮想閉域網識別子に基づき、該パケットの中継が許されている１つ以上の仮想閉域網を選択する手段と、前記１つ以上の仮想閉域網に対応する１つ以上の経路ドメインを選択する手段と、前記パケットの送信先アドレスと前記１つ以上の経路ドメインの各経路ドメイン情報とを照合して前記パケットを次のパケット中継装置に送出するための送出先アドレス（次ポップルータアドレス）を選択する手段と、前記送出先アドレスに前記パケットを送出する手段を有することを特徴とする。

【００３５】

また、本発明のパケット中継方法は、入力されたパケットの送信元仮想閉域網識別子に基づき、該パケットの中継が許されている１つ以上の仮想閉域網を選択するステップと、前記１つ以上の仮想閉域網に対応する１つ以上の経路ドメインを選択するステップと、前記パケットの送信先アドレスと前記１つ以上の経路ドメインの各経路情報（ｄｅｓｔｉｎａｔｉｏｎ）とを照合し、前記パケットの送出先アドレス（次ポップルータアドレス）を選択するステップと、前記送出先アドレスに前記パケットを送出するステップを有することを特徴とする。

【００３６】

また、本発明のパケット中継装置は、複数の送信元ＶＰＮ識別子（送信元仮想閉域網識別子）と該各送信元ＶＰＮ識別子に対応する１つ以上の宛先ＶＰＮ識別子（宛先仮想閉域網識別子）を管理するポリシ管理部（ＶＰＮ間中継ポリシ実施部）と、前記ポリシ管理部から1つ以上の送信元ＶＰＮ識別子（送信元仮想閉域網識別子）と該１つ以上の各送信元ＶＰＮ識別子（送信元仮想閉域網識別子）に対応する１つ以上の宛先ＶＰＮ識別子（宛先仮想閉域網識別子）を該１つ以上の各送信元ＶＰＮ識別子（送信元仮想閉域網識別子）に対応させて端末に表示する表示部（構成情報設定表示部）とを備えることを特徴とする。

【００３７】

また、本発明のパケット中継装置は、各宛先ＶＰＮ識別子（宛先仮想閉域網網識別子）と該各宛先ＶＰＮ識別子に対応する１つ以上の経路ドメイン識別子を管理する仮想閉域網管理部（ＶＰＮ定義部）を備え、前記仮想閉域網管理部は端末から入力される１つの宛先ＶＰＮ識別子と該１つの宛先ＶＰＮ識別子に対応する１つ以上の経路ドメイン識別子を対応させて前記端末に表示する表示部（構成情報設定表示部）とを備えることを特徴とする。

【００３８】

また、本発明のパケット中継装置は、端末からの指示に基づきドメイン間中継ポリシテーブルに設定された各送信元ＶＰＮ識別子（送信元仮想閉域網識別子）および前記各送信元ＶＰＮ識別子に対応する経路ドメインの一覧を要求する手段と、前記要求に基づいてドメイン間中継ポリシテーブルから１つ以上の送信元ＶＰＮ識別子（送信元仮想閉域網識別子）を抽出し、前記各送信元ＶＰＮ識別子に対応する経路ドメインの一覧を抽出する手段と、抽出された前記各送信元ＶＰＮ識別子および前記各送信元ＶＰＮ識別子に対応する経路ドメインの一覧を前記端末に表示する手段を備えることを特徴とする。

【００３９】

【発明の実施の形態】

以下、図面を参照しながら本発明の動作原理および好適な実施の態様を説明する。なお、以降、送信元ＶＰＮ識別子を仮想閉域網識別子と呼び、宛先ＶＰＮ識別子を宛先仮想閉域網識別と呼び、送信先ＶＰＮ識別子を送信先仮想閉域網識別子と呼ぶことがある。また、送信元ＶＰＮ識別子を送信元ＶＰＮ、送信先ＶＰＮ識別子を送信先ＶＰＮ、経路ドメインをドメインと呼ぶことがある。

【００４０】

図４は本発明の中継装置１００の動作原理を説明する図である。

【００４１】

図中、パケット中継手段５１は、入力されたルーティングパケットを経路情報管理手段５４に送出し、入力されたパケットをドメイン間中継手段５３、ネットワーク間中継手段５２及び経路情報管理手段５４との連携により得られた情報に基づき中継の対象となるパケットを所望の転送先に送出する。なお、ルーティン

グパケットに含まれるルーティング情報に依存せずに、手作業によりルーティング情報を経路情報管理手段５４に設定してもよい。また、ネットワーク間中継手段５２は１つ以上の経路ドメインを収容する仮想閉域網（ＶＰＮ）を対象にしてもよい。

【００４２】

前記ネットワーク間中継手段５２は、パケット中継手段５１から呼び出され、パラメタとしてパケットのヘッダ情報および属性情報を受け取る。次に、該パケットに対応する送信元仮想識閉域網識別子（送信元ＶＰＮ識別子）に基づき中継可能な仮想識閉域網識別子（送信先ＶＰＮ識別子）を検索する。

【００４３】

そして、ドメイン間中継手段５３を呼び出す。そのときに該パケットのヘッダ情報、属性情報、および中継可能な仮想識閉域網識別子（送信先ＶＰＮ識別子）をパラメタとして渡す。ドメイン間中継手段５３は、中継可能な仮想識閉域網が収容される各経路ドメインを特定し、送信先ＩＰアドレスに基づき所望の転送先ＩＰアドレスおよび出力インタフェース情報等、あるいは、中継できない旨の情報を経路情報管理手段５４から取得する。それらの情報を最終的にパケット中継手段５１に通知する。パケット中継手段５１は前記情報に基づき前記パケットを所望の転送先に送出する、あるいは、破棄する。

<実施の態様１>

図５は、本発明の第１の実施態様の例を説明する図である。

【００４４】

受信インタフェース１３は、接続されたネットワーク（例えば、ＬＡＮ、ＷＡＮ又はインターネット）からパケットを受信し、それをパケット受信部１０に送出する。

【００４５】

送信元ＶＰＮ識別テーブル９は、前記受信インタフェース１３を介して受信したパケットの送信元ドメインおよび送信元ＶＰＮを識別するためのテーブル（テーブル形式の例は後述する）である。

【００４６】

パケット受信部１０は、前記ネットワークから前記受信インタフェース１３を介して受信したＩＰパケットのヘッダに設定されている送信先ＩＰアドレスを解析し、このパケットを中継するか、あるいは自局（自ルータ）で受信するかを判定する。

【００４７】

また、パケット受信部１０は、このパケットを受信した受信インタフェース１３の識別子(例えば、ポート番号)をキーとして、送信元ＶＰＮ識別テーブル９を検索し、このＩＰパケットがどの経路ドメインおよびどのＶＰＮから受信したか識別する。なお、送信元ＶＰＮ識別テーブル９に送信元ＩＰアドレスフィールドを追加すれば、前記検索キーとしてＩＰパケットヘッダの送信元ＩＰアドレスを用いても同様な結果を得ることができる。

【００４８】

パケット受信部１０は、自局宛のルーティングパケット（例えば、経路情報を含むＢＧＰ－４［ｂｏｒｄｅｒ　ｇａｔｅｗａｙ　ｐｒｏｔｏｃｏｌ　ｖｅｒｓｉｏｎ　４］パケット等）を受信した場合には、それを経路情報処理部１に送出する。受信したパケットが他の中継装置に中継するパケットである場合にはパケット中継部１１に送出する。なお、他の自局宛データパケットについては当業者にとって既知であるので説明を省略する。

【００４９】

経路情報処理部１は複数のドメイン内中継テーブル４を有し、通常、ルータが管理する経路ドメインの数に対応して存在する。経路情報処理部１は、パケット受信部１０を介して経路情報（ルーティング情報）を含むパケットを受信し、その経路情報の属する経路ドメイン（送信元ＶＰＮ識別テーブル９から判別される）に対応するドメイン内中継テーブル４(テーブル形式の例は後述する)を更新する。

【００５０】

例えば、パケット受信部１０は、受信したパケットの受信インタフェース１３から送信元ＶＰＮ識別テーブル９を参照し、送信元の経路ドメインを特定する。そして、特定した経路ドメイン情報と受信した経路情報を経路情報処理部１に送

出する。

【００５１】

経路情報処理部１では、パケット受信部１０で特定した経路ドメインに基づき対応する１つのドメイン内経路情報管理部２を選択する。選択されたドメイン内経路情報管理部２は前記経路ドメイン情報に対応するドメイン内中継テーブル４を前記経路情報に基づき更新する。なお、中継装置１００に設定された経路情報はパケット送信部１２を介して他の中継装置（ルータ等）に配布される。

【００５２】

各ドメイン内中継テーブル４は、経路ドメインに対応して存在し、経路ドメイン内でのパケットの中継（ルーティング）に必要な経路情報を管理するテーブルである。この各ドメイン内中継テーブル４は手作業により構築してもよい。各ドメイン内中継テーブル４を手作業により構築した場合はドメイン内経路情報管理部１を省略することができる。

【００５３】

パケット中継部１１は、前記パケット受信部１０から受信したパケットを他の中継装置に中継するのに必要な情報を得るためにＶＰＮ間中継ポリシ実施部６、ＶＰＮ定義部５、および各ドメイン内中継テーブル４との連携を行い、出力パケットのヘッダ情報の生成、送信インタフェース１４での出力インタフェースを決定し、パケット送信部１２へ出力パケットを送出する。

【００５４】

更に詳細には、パケット中継部１１は、中継するパケットの送信元経路ドメイン、送信元ＶＰＮ識別子（送信元仮想閉域網識別子）および送信先ＩＰアドレスを呼び出しパラメタにしてＶＰＮ間中継ポリシ実施部６を呼び出す。

【００５５】

ＶＰＮ間中継ポリシ実施部６は、送信元ＶＰＮ識別子（送信元仮想閉域網識別子）と送信先ＶＰＮ識別子との接続関係（対応関係）を管理するとともに、ＶＰＮ間中継ポリシテーブル８を前記ＶＰＮ識別子及び前記送信先ＩＰアドレスを用いて検索し、このパケットを中継できる各ＶＰＮ識別子の一覧および該各ＶＰＮ識別子に付帯するＩＰアドレス情報を取得する。

【００５６】

図示していないが、例えば、前記パケットの送信元のＶＰＮ識別子がＶＰＮ＃１であり、このＶＰＮ＃１に対応する中継可能なＶＰＮ識別子として、ＶＰＮ＃１，ＶＰＮ＃２，ＶＰＮ＃４がＶＰＮ間中継ポリシテーブル８に定義されているとすれば、ＶＰＮ間中継ポリシ実施部６はＶＰＮ＃２，ＶＰＮ＃１，ＶＰＮ＃４を取得する。

【００５７】

このとき、ＶＰＮ＃２の優先順位が一番高く、ＶＰＮ＃４が一番低いものとする。また、ＶＰＮ＃１に付帯するＩＰアドレス情報として１０．１００．１２３．０／２４と定義されていれば、このＩＰアドレス情報も取得できる。このＩＰアドレス情報は１つ以上でもよい。また、ＩＰアドレス情報に論理積（ＡＮＤ）、論理和（ＯＲ）、論理否定（ＮＯＴ）、括弧などの論理演算子等、および／または、接続に関する指示（例えば、許可［Ｐｅｒｍｉｔ］、不許可［Ｄｅｎｙ］）等を含めて表現してもよい。

【００５８】

即ち、前記パケットを中継可能なＶＰＮ識別子が得られ、その、ＶＰＮ識別子に付帯する条件として、ＩＰアドレス情報を指定できる。これは、例えば、パケットをＶＰＮ＃２に中継可能であっても、付帯条件として指定されたＩＰアドレス情報が指定された条件に合致しなければそのパケットの中継はできないことになる。例えば、パケットの宛先ＩＰアドレスが10.10.50.50であった場合、前述のＩＰアドレス情報として「10.10.50.0/24　Deny」と指定されていれば、ＶＰＮ＃２として中継可能であるが、前記ＩＰアドレス情報によれば該パケットは中継できないことになる。

【００５９】

次に、ＶＰＮ間中継ポリシ実施部６（図５）はパケット中継部１１から受け取った前記送信先ＩＰアドレス、前記送信元経路ドメイン、及びＶＰＮ間中継ポリシテーブル８から取得した１つ以上の各送信先ＶＰＮ識別子と該各送信先ＶＰＮ識別子に付帯するＩＰアドレス情報をパラメタにしてＶＰＮ定義部５（図５）を呼び出す。

【００６０】

前記ＶＰＮ定義部５は、送信先ＶＰＮ識別子と経路ドメイン識別子との接続関係（対応関係）を管理するとととともに、パラメタとして受け渡された前記各送信先ＶＰＮ識別子に対応するドメイン間中継ポリシテーブル７を参照し各ドメイン内中継テーブル４にそれぞれ優先順位を付与する。そして、パラメタとして受け渡された前記送信先ＩＰアドレスを用いて各ドメイン内中継テーブル４を前記優先順位にしたがって検索する。このとき、各送信先ＶＰＮ識別子に付帯するＩＰアドレス情報も評価する。この検索結果において、最初に検出された次ホップルータのＩＰアドレス及び出力インタフェースの情報、あるいは、中継できない（検索の結果、該当する情報を得られなかった）といった情報を得る。なお、ドメイン間中継ポリシテーブル７から中継ポリシとしてフィルタリング情報、アドレス変換のＮＡＴ(Network Address Translation)情報なども得ることができる。

【００６１】

そして、これらの情報をＶＰＮ間中継ポリシ実施部６およびパケット中継部１１を介してパケット送信部１２に渡す。このとき、パケット中継部１１は、中継できないとの情報を受ければ該パケットを破棄する。

【００６２】

パケット送信部１２はこのパケットを送信すべき次ホップルータのＩＰアドレス及び出力インタフェースの情報を受け取るとパケット中継部１１からパケットのヘッダ情報の付け替え（送信先ＩＰアドレスの付与等）を行い、関連する送信インタフェース情報（出力インタフェース等）を送信インタフェース１４に送出する。

【００６３】

なお、経路情報処理部１から経路情報を含むパケットを受信した場合は該パケットを指定された送信インタフェース１４に送出する。この技術は既知なので詳細は省略する。

【００６４】

送信インタフェース１４は、前記送信インタフェース情報に基づき出力インタフェースに合わせてパケット送信部１２から受信したパケットを送出する。そし

て、この中継装置に接続されたネットワークに送出される。

【００６５】

以上の説明により、ＶＰＮ間中継ポリシテーブル８に設定された送信先ＶＰＮ識別子と送信先ＶＰＮ識別子との接続可否に関するポリシ、及びドメイン間中継ポリシテーブル７に設定された送信先ＶＰＮ識別子と経路ドメインとの接続可否に関するポリシに基づいてパケットの中継可否を容易に処理することができる。

【００６６】

また、ドメイン間中継ポリシテーブル７およびＶＰＮ間中継ポリシテーブル８が階層構造に構成されているので、前記ポリシの設定／変更が容易にできる。

<実施の態様２>

図６は本発明の第２の実施態様の例を説明する図である。

【００６７】

第１の実施態様（図５）と第２の実施態様（図６）との本質的な差異は経路情報処理部１に経路フィルタ３を設けることにある。経路フィルタ３は、ドメイン内経路情報管理部２がドメイン内中継テーブル4に設定する経路情報を制限（フィルタリング）するためのフィルタである。

【００６８】

例えば、図６に示す例では、経路フィルタ３を１つの経路ドメインに対してのみ設けているが、経路情報処理部1において複数または全てのドメイン内経路情報管理部２に対応して設けてもよい。

【００６９】

この経路フィルタ3はドメイン内経路情報管理部２から対応するドメイン内中継テーブル４に経路情報を設定するが，その際、経路フィルタ３が介在している場合は、この経路フィルタで指定された条件の経路情報のみを通過させる。

【００７０】

経路フィルタ３にＩＰアドレスとして、例えば、１９２．１６９．３０．０／２４が指定された場合、全３２ビット中、先頭ビットから２４ビット（ＩＰアドレスの最後に「／２４」を付加して記述する）と一致するＩＰアドレス（１９２．１６９．３０．＊）［＊は０～２５５の任意値を示す］）に関する経路情報の

設定を明示的に禁止する、あるいは、前記ＩＰアドレスのみの設定を許可することにより、この経路フィルタで許可された経路情報のみをドメイン内経路情報管理部２に設定することができる。

【００７１】

このようにして、１つの経路ドメインに対して経路フィルタ３により上位ｎビット（前述の例では先頭２４ビット）を用いてＩＰアドレスを１つ以上にグループ化し、そのグループの論理和などの処理を行うことにより、同一ドメイン内のポリシの設定において、更に細かなＩＰアドレスのグルーピングによるポリシの設定が可能になる。

<実施の態様３>

第３の実施態様は第２の実施態様の変形例の１つであり、図７は、本発明の第３の実施態様の例を説明する図である。

【００７２】

第３の実施態様（図７）と第２の実施態様（図６）との本質的な差異は、経路フィルタ３Ａにより分割された複数のドメイン内中継テーブル４Ａを対応させて経路情報を設定できる点にある。

【００７３】

すなわち、あるＩＰアドレスグループを有する１つの経路ドメインを２つ以上に分割して運用する場合、経路情報処理部１の対応するドメイン内経路情報管理部２に経路フィルタ３Ａを設けることにより少ない作業量で、分割された経路ドメインに対応する複数のドメイン内中継テーブル４を効率的に構築することができる。

【００７４】

例えば、一つの経路ドメインを２つの経路ドメインに分割して新たな運用を行う場合、分割された各経路ドメインに対応する２つのＩＰアドレスグループがあるとする。図示していない第１グループのＩＰアドレスは、１９２．１６８．１０．０／２４であり、第２グループは１９２．１６８．２０．０／２４とする。

【００７５】

このような場合、経路フィルタ３Ａにより第１グループの経路情報をドメイン

内中継テーブル４Ａに設定し、第２グループの経路情報を対応するドメイン内中継テーブル４Ｂに設定することができる。

【００７６】

このように、１つの経路ドメインを２つ以上の経路ドメインに分割した場合には、上述のようにＩＰアドレスグループ単位に対応する複数のドメイン内中継テーブル４に経路情報の設定を制御することができる。

<実施の態様４>

第４の実施態様は第１の実施態様の変形であり、図８に本発明の第４の実施態様の例を説明する図を示す。

【００７７】

第４の実施態様（図８）と第１の実施態様（図３）との本質的な差異は、ＶＰＮ定義部５と構成情報設定表示部１５との連携、およびＶＰＮ間中継ポリシ実施部６と構成情報設定表示部１５との連携にある。

【００７８】

すなわち、構成情報設定表示部１５に接続された端末１６（例えば、ワークステーションなど）からの指令に基づきドメイン間中継ポリシテーブル７及びＶＰＮ間中継ポリシテーブル８に設定された情報を端末１６から指定された条件に基づいて表示／更新（変更、追加、削除）することにある。

【００７９】

この端末１６は回線（ＷＡＮ、ＬＡＮ、インターネットあるいは電話回線等）を介して接続されたリモート端末（例えば、ＰＣ等）であってもよい。

【００８０】

詳細には、構成情報設定表示部１５は、構成情報設定表示部１５に接続された端末１６からのコマンド等の指令により、ＶＰＮ間中継ポリシテーブル８に定義された各送信元ＶＰＮ識別子（送信元仮想閉域網識別子）および該各送信元ＶＰＮ識別子に対応する送信先ＶＰＮ識別子（送信先仮想閉域網識別子）の一覧の要求をＶＰＮ間中継ポリシ実施部６に依頼する。

【００８１】

ＶＰＮ間中継ポリシ実施部６はその要求に基づいて、ＶＰＮ間中継ポリシテー

ブル８を参照し、設定されているすべてのＶＰＮ識別子を検索し、各送信元ＶＰＮ識別子（送信元仮想閉域網識別子）に対応する送信先ＶＰＮ識別子の一覧を構成情報設定表示部１５に渡す。

【００８２】

そして、端末１６に図９に示す送信元ＶＰＮの一覧を表示するメニー（ウインドウ）の例を表示する。

【００８３】

端末１６の画面（ウインドウ）から特定の送信先ＶＰＮ識別子が入力された場合、例えば、図９に図示された送信元ＶＰＮとして「ＶＰＮ２」をクリックした場合には「送信元ＶＰＮ２」が構成情報設定表示部１５に入力される。

【００８４】

構成情報設定表示部１５は、送信元ＶＰＮ２に対応する宛先ＶＰＮ（送信先ＶＰＮ）に関する情報の取得をＶＰＮ間中継ポリシ実施部６に依頼する。

【００８５】

ＶＰＮ間中継ポリシ実施部6は、指定された送信元ＶＰＮ識別子（送信元仮想閉域網識別子）である「ＶＰＮ２」に対応する宛先ＶＰＮ識別子（送信先仮想閉域網識別子）を求めるためにＶＰＮ間中継ポリシテーブル８を検索し、その結果を構成情報設定表示部１５に通知する。

【００８６】

構成情報設定表示部１５は通知された宛先ＶＰＮ識別子の数が１つ以上であれば、その各宛先ＶＰＮ識別子に対応する送信先経路ドメインの検索をＶＰＮ定義部５に依頼する。ＶＰＮ定義部５は前記各宛先ＶＰＮ識別子に基づきＶＰＮ間中継ポリシテーブル7を検索し、対応する各経路ドメイン識別子を取得する。

【００８７】

その取得結果をＶＰＮ定義部５に通知する。ＶＰＮ定義部５は構成情報設定表示部１５に、各宛先ＶＰＮ識別子および各経路ドメイン識別子を対応づけて通知する。構成情報設定表示部１５は、前記送信元ＶＰＮ識別子とそれに対応する各宛先ＶＰＮ識別子、及び該各宛先ＶＰＮ識別子に対応する各経路ドメイン識別子をＧＵＩ（Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）として端末１

６の画面上に表示する。前記画面のウインドウに表示する例を図１０に示す。

【００８８】

なお、前述の説明では、端末画面上への表示を中心に説明したが、表示した情報（送信元ＶＰＮ識別子，宛先ＶＰＮ識別子（送信先ＶＰＮ識別子），送信先経路ドメイン識別子）に対する追加、変更、削除の方法について説明する。

【００８９】

例えば、送信元ＶＰＮ識別子(送信元仮想閉域網識別子)を追加登録する例を説明する。

【００９０】

端末１６の画面上に図９に示すメニー（ウィンドウ）が表示されている状態において、ファンクションキー（ＰＦ１～ＰＦ１２）のうち、例えば、ＰＦ５を押下すると、「ＶＰＮ３」と表示されている下に、新たな送信元ＶＰＮ識別子を追加登録するための入力を指示が、例えば、図１１のように表示される。

【００９１】

その指示に従って追加登録すべき送信元ＶＰＮ識別子が入力された場合、構成情報設定表示部１５はこの入力に基づきＶＰＮ間中継ポリシ実施部６に前記送信元ＶＰＮ識別子の追加処理を依頼する。そして、ＶＰＮ間中継ポリシ実施部６はＶＰＮ間中継ポリシテーブル８に前記送信元ＶＰＮ識別子の追加登録を行う。そして、端末１６は次の指示入力待ち状態となる。

【００９２】

送信元ＶＰＮ識別子の削除は、例えば、図９に表示されている状態において、ＰＦ６キーを押下することにより、例えば、図１２に示すメニューが表示される。

【００９３】

そして、削除すべき送信元ＶＰＮ識別子が入力された場合には、構成情報設定表示部１５はこの指示に基づきＶＰＮ間中継ポリシ実施部６に指定された送信元ＶＰＮ識別子の削除を依頼する。そして、ＶＰＮ間中継ポリシ実施部６はＶＰＮ間ＶＰＮ間中継ポリシテーブル８に前記送信元ＶＰＮ識別子の削除を行う。そして、端末１６は次の指示入力待ち状態となる。

【００９４】

送信元ＶＰＮ識別子の変更は、例えば、図９に表示されている状態において、例えば、カーソルを変更したい送信元ＶＰＮ識別子の上に置き、そしてＰＦ７キーを押下することにより、例えば、図１３に示すメニュー（ウインドウ）が表示される。

【００９５】

また、送信元ＶＰＮ識別子の変更指示が入力された場合には、構成情報設定表示部１５はこの指示に基づきＶＰＮ間中継ポリシ実施部６に，変更前の現送信元ＶＰＮ識別子と変更後の新送信元ＶＰＮ識別子をパラメタにして変更を依頼する。

【００９６】

構成情報設定表示部１５はこのパラメタに基づきＶＰＮ間中継ポリシ実施部６に指定された現送信元ＶＰＮ識別子を新送信元ＶＰＮ識別子に変更する処理を依頼する。そして、ＶＰＮ間中継ポリシ実施部６はＶＰＮ間中継ポリシテーブル８の現送信元ＶＰＮ識別子の変更を行う。そして、端末１６は次の指示入力待ち状態となる。

【００９７】

構成情報設定表示部１５は、端末１６から宛先ＶＰＮ識別子（図１０の右側）の追加／削除／変更の入力を受信した場合には、構成情報設定表示部１５はこの指示に基づきＶＰＮ間中継ポリシ実施部６に指定された宛先ＶＰＮ識別子の一覧の更新（追加、削除、または変更）処理を依頼する。

【００９８】

図示していないが、これらの宛先ＶＰＮ識別子の変更処理の依頼も前述と同様にＰＦキー８（追加）、変更の対象となる宛先ＶＰＮ識別子の上にカーソルを置いてＰＦキー９（削除）を押下、変更の対象となる宛先ＶＰＮ識別子の上にカーソルを置いてＰＦキー１０（変更）を使用することにより、同様に、構成情報設定表示部１５はＶＰＮ間中継ポリシ実施部６に前記宛先ＶＰＮ識別子の更新（追加、削除または変更）を依頼する。

【００９９】

ＶＰＮ間中継ポリシ実施部６は前記依頼に基づいてＶＰＮ間中継ポリシテーブル８の更新（追加、削除、または変更）を行う。

【０１００】

図１４は，図９に示すメニュー（ウインドウ）において送信元ＶＰＮ３をクリックした場合に表示される情報の例であり、主たる情報の構造は図１０と同じある。しかしながら、図１４には属性情報１～４が表示されているが、図１０には表示されていない点で異なる。なお、属性情報１～４は、初期画面に表示されていない。

【０１０１】

これらの属性情報は、送信元ＶＰＮ識別子または宛先ＶＰＮ識別子にカーソル移動する、あるいは、それをクリックするとそのＶＰＮ識別子に関する属性情報が端末１６に表示される。

【０１０２】

より詳細には、例えば、端末１６の画面上に表示された送信元ＶＰＮ識別子（ＶＰＮ３）、宛先ＶＰＮ識別子（ＶＰＮ３，ＶＰＮ１）、ドメイン名（ドメイン４，ドメイン１、及びドメイン２）の上にカーソルを移動させると、構成情報設定表示部１５にカーソルがその表示対象に移動したことが通知される。

【０１０３】

構成情報設定表示部１５は通知された情報に基づきＶＰＮ識別子を特定する。例えば、特定された対象が送信元ＶＰＮ３であるとすれば、該ＶＰＮ３に関する属性情報１を前述したようにＶＰＮ間中継ポリシテーブル８を検索し、取得した属性情報１を画面上に表示する。

【０１０４】

同様に、属性情報２の表示では、構成情報設定表示部１５は通知された指示にしたがって、宛先ＶＰＮ２をパラメタとしてＶＰＮ定義部５を呼び出し、対応する属性情報２の抽出を依頼する。そして、ＶＰＮ定義部５は属性情報２を抽出し構成情報設定表示部１５に通知する。

【０１０５】

構成情報設定表示部１５は、通知された宛先ＶＰＮ２の属性情報２を端末１６

に表示する。端末装置１６における表示の例を図１４に示す。

【０１０６】

更に、構成情報設定表示部１５が端末１６に属性情報２を表示中に、例えば、ＰＦ１１キーを押下すると表示名の属性情報２を更新することができる状態になる。

【０１０７】

表示された属性情報２の各項目の変更は、上書きすることにより変更することができる。例えば、宛先アクセス優先度１の右側に「ドメイン４」と値が表示されているが、これを、「ドメイン３」と設定し直す（タイプインする）と「ドメイン４」を「ドメイン３」に変更することができる。

【０１０８】

また、削除キーを使って、表示された「ドメイン４」を削除する、あるいは、空白により上書きすると、「ドメイン４」は削除される。

【０１０９】

また、ＰＦ１２キーを押下すると、「ドメイン４」の下に新たな入力フィールドが現れ、追加登録すべき送信先経路ドメインの入力が可能になる。この入力フィールドに、例えば、「ドメイン５」を入力すると、既に設定されている「ドメイン４」の他に「ドメイン５」を追加登録することができる。

【０１１０】

同様に、Ｏｗｎｅｒ，アクセスルール、フィルタ条件の各フィールド値も変更することができる。

【０１１１】

また、端末１６の画面（ウインドウ）から送信先経路ドメインの編集（追加、削除、または変更）を想定する。例えば、図１１に図示された「ドメイン４」を端末１６のウインドウ上に表示された宛先ＶＰＮ３配下の「ドメイン４」をクリックした場合には「宛先ＶＰＮ３のドメイン４」が構成情報設定表示部１５に入力される。

【０１１２】

構成情報設定表示部１５は、「宛先ＶＰＮ３のドメイン４」をパラメタとして

、ＶＰＮ定義部５に属性情報３の取得を依頼する。ＶＰＮ定義部５はドメイン間中継ポリシテーブル７から送信先ＶＰＮ識別子である宛先ＶＰＮ３およびドメイン４の属性情報３を取得し、構成情報設定表示部１５に通知する。

【０１１３】

構成情報設定表示部１５は、通知された属性情報３を端末１６に表示する。表示の例を図１１の右上に示す。

【０１１４】

図１５は送信元ＶＰＮ識別子に関する情報（送信元ＶＰＮ識別子、送信先ＶＰＮ識別子、経路ドメイン識別子）を既に説明した同様な手順により取得できることは明らかである。よって、ここでは、図１５を使ってその情報の表示方法を説明する。

【０１１５】

図中、３つウインドウが表示されており、ウインドウ１がルートウインドウであり、図９に示す画面表示内容と同じ表示内容である。ウインドウ２はウインドウ１内に表示されている送信元ＶＰＮ識別子の内表示対象（この図ではＶＰＮ３）を左クリックするとウインドウ２が新たに表示される。右クリックすると属性情報１が表示される。

【０１１６】

ウインドウズ２が表示された状態で表示対象（この図では上段の宛先ＶＰＮ３）を右クリックすると属性情報２が表示される。一方、左クリックするとウインドウ３が新たに表示され、そのウインドウ内に前記宛先ＶＰＮ３に対応する経路ドメイン４が表示される。

【０１１７】

ウインドウ３の経路ドメイン４を右クリックすると属性情報３が表示される。

【０１１８】

以上のように階層的に、例えば、ウインドウ１～３のように、送信元ＶＰＮ識別子、宛先ＶＰＮ識別子（送信先ＶＰＮ識別子）、宛先（送信先）経路ドメイン識別子の関係を階層的に端末１６に表示することにより、送信元ＶＰＮに関連する設定情報を容易に確認することができる。

【０１１９】

特に、ＧＵＩを介して前記階層化された送信元ＶＰＮ識別子に対応する情報を視覚的に整理された情報として端末画面上に表示することができる。なお、情報が多い場合には１つのウインドウ（論理画面）を複数の物理画面（端末画面）に分割して個々を１画面として表示する、あるいは、スクロール機能により連続的移動表示することにより、全体情報を容易に把握することができる。

【０１２０】

以上のように、ドメイン間中継ポリシテーブル７およびＶＰＮ間中継ポリシテーブル８の情報を端末１６に表示／更新することにより設定情報を容易に確認することができる。更に、確認した設定情報を変更したい場合には、その値を確認しながら変更、追加、削除を容易に行うことができる。

<実施の態様５>

図１６は本発明の第１の実施態様を適用したルータをプロバイダが提供するネットワークに採用した例を説明する図である。なお、この実施例では、プロバイダが提供するＶＰＮサービスと同等なＶＰＮサービスをキャリアが提供する場合、該キャリアは該プロバイダに含まれるものとする。

【０１２１】

図１７は図１６に示すネットワークのドメイン構成を説明する図である。

【０１２２】

図１８は図１６に示すルータ１における受信インタフェースと送信元ドメイン及び送信元ＶＰＮとの対応を管理する送信元ＶＰＮ識別テーブル9の例を説明する図である。

【０１２３】

図１９はＶＰＮ間の中継ポリシを設定するテーブルの形式の例を説明する図である。

【０１２４】

図２０はドメイン間中継ポリシを設定するテーブルの形式及び設定値の例を説明する図である。図２１、図２２および図２３は経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【０１２５】

図１６乃至図２３を参照しながら本発明を適用したルータの動作例を説明する。

【０１２６】

図１６に示すプロバイダ網がＶＰＮサービスを提供するネットワークには、４つの経路ドメイン（ドメイン＃１～ドメンイ＃４）が存在し、３つルータ（ルータ１～ルータ３）が存在している。

【０１２７】

このうちドメイン＃１，＃２，＃４を管理しているルータ1（ＩＰアドレスは192.168.254.1）に着目して、本発明を適用したルータ1の動作例を説明する。なお、ルータ２またはルータ３は本発明を適用してなくてもよいが、適用してもよい。まず、ＶＰＮサービスを提供するルータ1の一般的な動作を説明し、ＶＰＮ間および経路ドメイン間の接続性可否の処理説明は後述する。

【０１２８】

ルータ1は、収容する各経路ドメインに対応する各ドメイン内中継テーブルを備え、それぞれ独立に管理している。経路ドメイン＃１，＃２，＃４に対応させて構築した各ドメイン内中継テーブル４の形式の例を図２１～図２３に示す。

【０１２９】

ルータ1は、受信インタフェースIF0～IF2（図１６）からそれぞれパケットを受信するとパケット毎に送信元ＶＰＮ識別テーブル９（図１６）を参照し、その受信パケットが属する経路ドメインを調べ、その経路ドメインに対応するドメイン内中継テーブル４（図２１～図２３）を参照し，次に中継する次ホップルータのＩＰアドレスおよび出力インタフェースを求める。そして、そのパケットのヘッダを作成し、出力インタフェースIF10～IF12（図１６）の選択されたいずれかから次ホップルータに送出する。

【０１３０】

例えば、ルータ1が、受信インタフェースIF0（図１６）から送信先ＩＰアドレスが192.168.100.10（経路ドメイン＃２，ＶＰＮ＃１）であるデータパケットを受信すると、まず、ルータ１は送信元ＶＰＮ識別テーブル９（図１８）を参照し

、受信インタフェースIF0（図１６）から受信したパケットがドメイン＃２に属し、送信元ＶＰＮ識別子がＶＰＮ＃１であることを特定する。

【０１３１】

次に、ＶＰＮ間中継ポリシテーブル８を検索して得られた、送信元ＶＰＮ識別子から中継可能なＶＰＮであるＶＰＮ＃１を構成する経路ドメインをドメイン間中継ポリシテーブル７から検索し、ＶＰＮ＃１に対してはドメイン＃１およびドメイン＃２を取得する。

【０１３２】

次に、ＶＰＮ＃１と経路ドメインとの接続性を検索する。すなわち、ＶＰＮ＃１を検索キーとしてドメイン間中継ポリシテーブル７（図２０）を検索する。その結果、重複情報を削除し、ドメイン＃１およびドメイン＃２を得る。

【０１３３】

次に、送信先ＩＰアドレス（192.168.100.10）をキーとして、ドメイン＃１およびドメイン＃２に対応するドメイン内中継テーブル４（図２１，図２２）を優先順序に従って、図２１、次に図２２を検索する。この検索は、複数のプロセッサを使用して並列処理を行ってもよい。この検索の結果、最初に検出された次ホップルータアドレスを採用する。

【０１３４】

経路ドメイン２のドメイン内中継テーブル４（図２２）から次ホップルータのＩＰアドレスとして192.168.254.3および出力インタフェースとしてIF10を得る。すなわち、このパケットは中継可能である。

【０１３５】

そして、次ホップルータとしてルータ３（192.168.254.3）に前記パケットを送出する。

【０１３６】

また、本実施の態様では、例えば、プロバイダは図１６に示した経路ドメイン間での接続の許可／不許可を図１７に示すように接続性を定義しているものとする。経路ドメイン＃１(10.25.0.0)と経路ドメイン＃２(192.168.0.0)はＶＰＮ＃１として相互に接続性を持ち、プロバイダ網を介してエクストラネットを構成し

ている。また、経路ドメイン＃２(192.168.0.0)と経路ドメイン＃３(10.30.0.0)はＶＰＮ＃２として相互に接続性を持ち、プロバイダ網を介してエクストラネットを構成している。

【０１３７】

経路ドメイン＃１(10.25.0.0)と経路ドメイン＃３(10.30.0.0)は相互に通信できる接続性は定義されていない。また、経路ドメイン＃４(192.172.0.0)は単一の経路ドメインから成り、イントラネットとしてＶＰＮ＃３を構成している。

【０１３８】

上述のネットワークにおいて、例えば、ＶＰＮ＃１(経路ドメイン＃１と＃２とのエクストラネット接続)とＶＰＮ＃３(経路ドメイン＃４でのイントラネット接続)とのＶＰＮ間通信ポリシ(フィルタ条件、アドレス変換処理等)を定義するものとする。アドレス変換処理とは、イントラネット内のみで使用されるローカルＩＰアドレスを独自に割り当てて運用し、イントラネットとインターネット間でパケットが送信/受信されるときにイントラネット内のローカルＩＰアドレスとグローバルＩＰアドレスとを相互に変換する処理を示す。このアドレス変換については、ＩＥＴＦ（Internet Engineering Task Force）が標準化したＲＦＣ１６３１等で既に規定されているので、詳細はこれを参照されたい。

【０１３９】

次に、図１９はルータ１においてＶＰＮ＃１～ＶＰＮ＃３との間における中継ポリシの設定例を説明する図である。これによると、ルータ１は、ＶＰＮ＃１からパケットを受信した場合は、ＶＰＮ＃１は無条件でパケットを中継可能であるが、他のＶＰＮ（例えばＶＰＮ＃３など）パケットを中継することはできない。

【０１４０】

一方、ＶＰＮ＃３からパケットを受信したルータ１は、ＶＰＮ＃３には無条件でパケット中継することが可能である。しかしながら、送信先がＶＰＮ＃１である場合は、送信先アドレスとして192.172.10.0/24を有するパケットを排除するフィルタ処理（図６に示す経路フィルタ３により処理される）が示されている。

【０１４１】

まず、ＶＰＮ＃１及びＶＰＮ＃３を構成するドメイン間の中継ポリシを図２０

に示すように設定されるものとする。この設定によると、ＶＰＮ＃１は、ドメイン＃１とドメイン＃２との接続性を持ち、どちらのドメインへも無条件で中継可能(permit)であることを示している。このとき、ドメイン＃１の方をドメイン＃２より優先してドメイン内中継テーブルを参照することを示している。

【０１４２】

また、ＶＰＮ＃３については、ドメイン＃４（ルータ１のIF2とルータ２のIF2との接続）のみから構成され、ドメイン＃４内のパケット転送は無条件の中継が許可されていることを示している。

【０１４３】

以上、上述したように第１の実施態様を適用したルータをプロバイダ網に適用することにより、プロバイダはＶＰＮサービスをエンドユーザに提供することができる。

（付記１）　入力されたパケットに対応する送信元仮想閉域網識別子に基づき、該パケットの中継が許されている１つ以上の仮想閉域網を選択する手段と、

前記１つ以上の仮想閉域網に対応する１つ以上の経路ドメインを選択する手段と、

前記パケットの送信先アドレスと前記１つ以上の経路ドメインの各経路ドメイン情報とを照合し、前記パケットを次のパケット中継装置に送出するための送出先アドレス（次ポップルータアドレス）を選択する手段と、

前記送出先アドレスに前記パケットを送出する手段を有することを特徴とするパケット中継装置。

（付記２）　付記１記載において、

前記パケットの送信元仮想閉域網および前記１つ以上の仮想閉域網の少なくとも１つは仮想私設網であることを特徴とするパケット中継装置。

（付記３）　付記１記載において、

前記経路情報管理手段は経路情報をフィルタする経路フィルタを具備し、

前記経路フィルタにより選択された経路情報をドメイン内中継テーブルに設定することを特徴とするパケット中継装置。

（付記４）　付記１記載において、

前記経路情報管理手段は経路情報（ｄｅｓｔｉｎａｔｉｏｎ）をフィルタする経路フィルタを具備し、

ドメイン間パケット中継手段が管理するドメイン内中継テーブルに経路情報を設定するときに、前記経路情報を複数のドメイン内中継テーブルに分割して書き込むことを特徴とするパケット中継装置。

（付記５）　入力されたパケットの送信元仮想閉域網識別子に基づき、該パケットを中継できる１つ以上の仮想閉域網を選択するステップと、

前記１つ以上の仮想閉域網に対応する１つ以上の経路ドメインを選択するステップと、

前記パケットの送信先アドレス（次ポップルータアドレス）と前記１つ以上の経路ドメインの各経路情報（ｄｅｓｔｉｎａｔｉｏｎ）とを照合し、前記パケットの送出先アドレスを選択するステップと、

前記送出先アドレスに前記パケットを送出するステップを有することを特徴とするパケット中継方法。

（付記６）　複数の送信元仮想閉域網識別子と該各送信元仮想閉域網識別子に対応する１つ以上の宛先仮想閉域網識別子を管理するポリシ管理部（ＶＰＮ間中継ポリシ実施部）と、

前記ポリシ管理部から1つ以上の送信元仮想閉域網識別子と該１つ以上の各送信元仮想閉域網識別子に対応する１つ以上の宛先仮想閉域網識別子を該１つ以上の各送信元仮想閉域網識別子に対応させて端末に表示する表示部（構成情報設定表示部）と

を備えることを特徴とするパケット中継装置。

（付記７）　付記６記載において、

前記ポリシ管理部は、前記表示部が前記端末から受け取る１つの送信元仮想閉域網識別子に対応する１つ以上の宛先仮想閉域網識別子を前記表示部に送出し、

前記表示部は、前記１つの送信元仮想閉域網識別子と前記１つ以上の宛先仮想閉域網識別子を対応させて前記端末に表示することを特徴とするパケット中継装置。

（付記８）　前記各宛先仮想閉域網識別子と該各宛先仮想閉域網識別子に対応す

る１つ以上の経路ドメイン識別子を管理する仮想閉域網管理部（ＶＰＮ定義部）を備え、

前記仮想閉域網管理部は前記端末から入力される１つの宛先仮想閉域網識別子と該１つの宛先仮想閉域網識別子に対応する１つ以上の経路ドメイン識別子を対応させて前記端末に表示する表示部（構成情報設定表示部）と

を備えることを特徴とするパケット中継装置。

（付記９）　付記６記載において、

前記表示部は、前記端末から追加登録すべき送信元仮想閉域網識別子を受け取って前記ポリシ管理部（ＶＰＮ間中継ポリシ実施部）に追加の登録を依頼し、

前記ポリシ管理部は送信元仮想閉域網識別子をＶＰＮ間中継ポリシテーブルに登録することを特徴とするパケット中継装置。

（付記１０）　付記６記載において、

前記表示部は、前記端末から受け取った削除すべき送信元仮想閉域網識別子の削除を前記ポリシ管理部に依頼し、

前記ポリシ管理部は該送信元仮想閉域網識別子をＶＰＮ間中継ポリシテーブルから削除することを特徴とするパケット中継装置。

（付記１１）　付記６記載において、

前記表示部は、前記端末から受け取った名称を変更すべき現送信元仮想閉域網識別子と新送信元仮想閉域網識別子を前記ポリシ管理部に名称の変更を依頼し、

前記ポリシ管理部は、ＶＰＮ間中継ポリシテーブルに存在する前記現送信元仮想閉域網識別子の名称を新送信元仮想閉域網識別子に変更することを特徴とするパケット中継装置。

（付記１２）　端末からの指示に基づきドメイン間中継ポリシテーブルに設定された各送信元仮想閉域網識別子および前記各送信元仮想閉域網識別子に対応する経路ドメインの一覧を要求する手段と、

前記要求に基づいてドメイン間中継ポリシテーブルから１つ以上の送信元仮想閉域網識別子を抽出し、前記各送信元仮想閉域網識別子に対応する経路ドメインの一覧を抽出する手段と、

抽出された前記各送信元仮想閉域網識別子および前記各送信元仮想閉域網識別

子に対応する経路ドメインの一覧を前記端末に表示する手段を備えることを特徴とするパケット中継装置。

（付記１３）　端末からの指示により、ドメイン間中継ポリシテーブルに設定された各送信先仮想閉域網識別子および各送信先仮想閉域網識別子に対応する１つ以上の経路ドメイン識別子の一覧を要求する手段と、

前記要求に基づいて、ドメイン間中継ポリシテーブルからドメイン識別子を検索し、各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を抽出する手段と、

前記端末に各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を表示するとともに送信先仮想閉域網識別子の追加登録の指示を端末から受け取る手段と、

前記ドメイン間中継ポリシテーブルに前記端末から受け取った送信先仮想閉域網識別子の追加登録を行う手段を備えることを特徴とするパケット中継装置。

（付記１４）　端末からの指示により、ドメイン間中継ポリシテーブルに設定された各送信先仮想閉域網識別子および各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を要求する手段と、

前記要求に基づいて、ドメイン間中継ポリシテーブルを参照して設定されている送信先仮想閉域網識別子を検索し、各送信先仮想閉域網識別子に対応するドメイン識別子の一覧を作成する手段と、

各送信先仮想閉域網識別子に対応するドメイン識別子一覧を端末に表示するとともに該ドメイン識別子の一覧について、送信先仮想閉域網識別子の追加またはドメイン識別子一覧を削除する指示を受け取る手段と、

指示された該追加または該削除に基づき前記ドメイン間中継ポリシテーブルの更新を行う手段と

を備えることを特徴とするパケット中継装置。

【０１４４】

【発明の効果】

本発明によれば、複数の経路ドメイン間相互の中継ポリシを定義する際に、複数の経路ドメインをいくつかのグループに分け、グループ間の中継ポリシとして

定義することを可能にする。このことにより定義する中継ポリシの数が減るため、設定／変更を容易に行える。

【０１４５】

また、中継に必要な経路情報を格納する中継テーブルのサイズを小さくすることができる。

【図面の簡単な説明】

【図１】

シングルドメイン／マルチドメイン，イントラネット／エクストラネットの組み合わせによるネットワーク構成の例を説明する図である。

【図２】

マルチドメイン構成のリクストラネットＶＰＮを収容するルータの中継テーブルの構成例を説明する図である。

【図３】

マルチドメイン構成のエクストラネットＶＰＮを収容するルータの中継テーブルの構成例を説明する図である。

【図４】

本発明の動作原理を説明する図である。

【図５】

本発明の第１の実施態様の例を説明する図である。

【図６】

本発明の第２の実施態様の例を説明する図である。

【図７】

本発明の第３の実施態様の例を説明する図である。

【図８】

本発明の第４の実施態様の例を説明する図である。

【図９】

本発明の第４の実施態様の例における送信元ＶＰＮの表示の例を説明する図。

【図１０】

本発明の第４の実施態様の例における送信元ＶＰＮと宛先ＶＰＮ、宛先ドメイ

ンとの対応関係の表示の例を説明する図。

【図１１】

本発明の第４の実施態様の例における送信元ＶＰＮを追加するメニーの表示の例を説明する図。

【図１２】

本発明の第４の実施態様の例における削除すべき送信元ＶＰＮを入力するメニーの表示の例を説明する図。

【図１３】

本発明の第４の実施態様の例における内証を変更すべき送信元ＶＰＮを入力するメニーの表示の例を説明する図。

【図１４】

本発明の第４の実施態様の例におけるツリー構造によるＶＰＮ管理情報の表示の例を説明する図。

【図１５】

本発明の第４の実施態様の例におけるマルチウインドウによるＶＰＮ管理情報の表示の例を説明する図。

【図１６】

本発明の第１の実施態様を適用したルータをプロバイダが提供するネットワークに採用した例を説明する図である

【図１７】

図１６に示すネットワークのドメイン構成を説明する図である。

【図１８】

図１６に示すルータ１における受信インタフェースと送信元ドメイン及び送信元ＶＰＮ識別子との対応を管理する送信元ＶＰＮ識別テーブルの例を説明する図である。

【図１９】

ＶＰＮ間の中継ポリシを設定するテーブルの形式の例を説明する図である。

【図２０】

ドメイン間中継ポリシを設定するテーブルの形式及び設定値の例を説明する図

である。

【図２１】

経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【図２２】

経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【図２３】

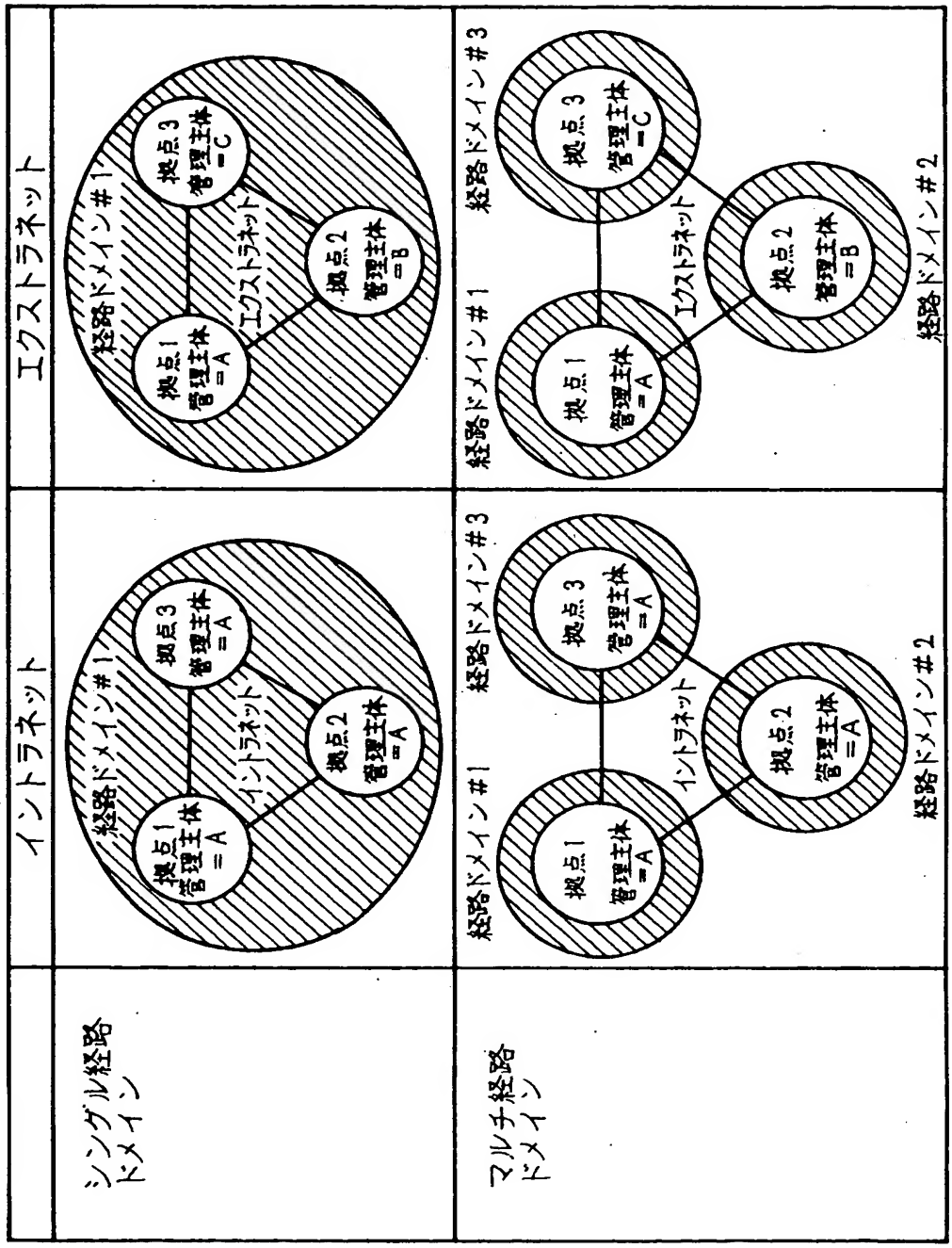
経路ドメイン間における中継テーブルの形式及び設定値の例を説明する図である。

【符号の説明】

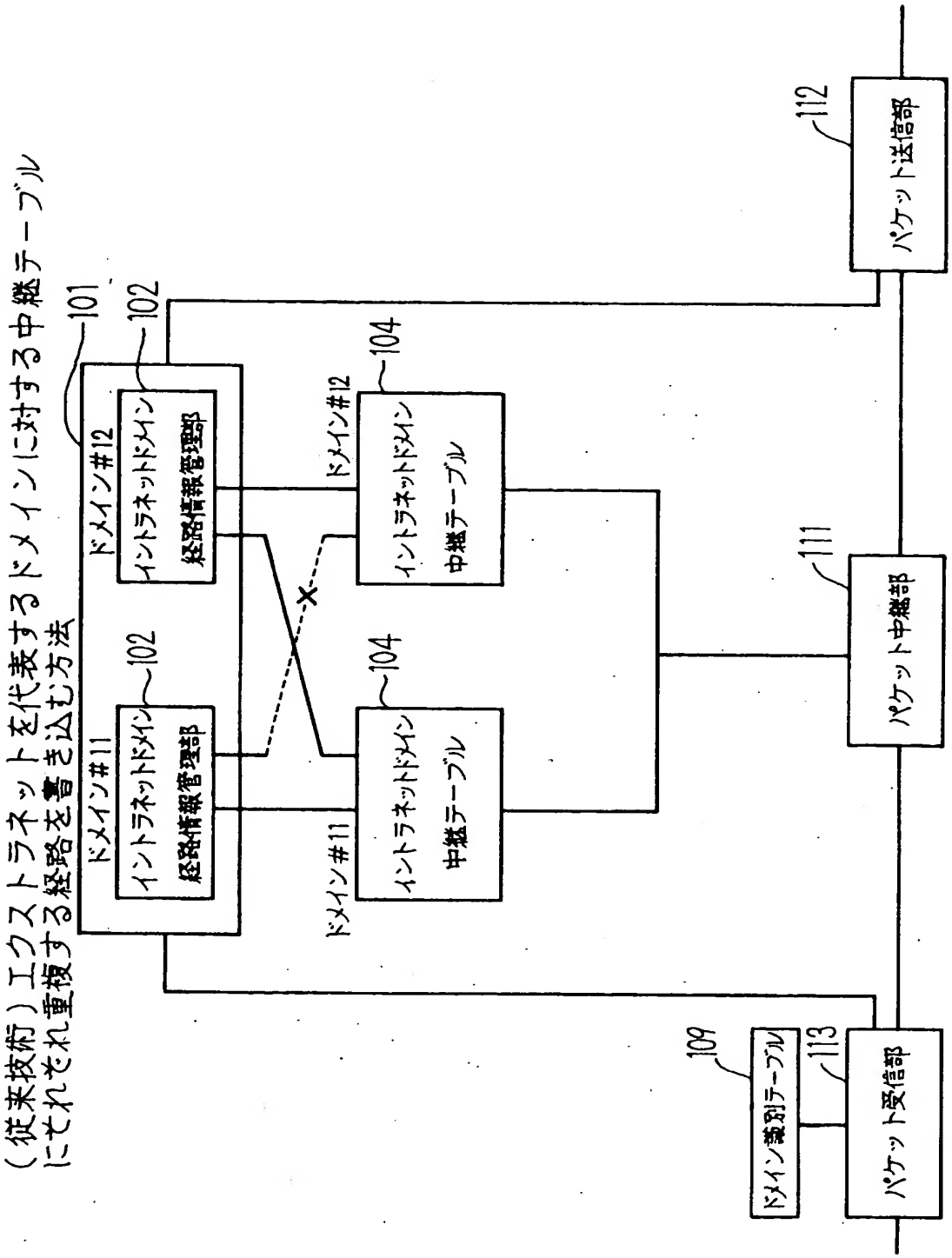
１　経路情報処理部
２　ドメイン内経路情報管理部
３　経路フィルタ
４　ドメイン内中継テーブル
５　ＶＰＮ定義部
６　ＶＰＮ間中継ポリシ実施部
７　ドメイン間中継ポリシテーブル
８　ＶＰＮ間中継ポリシテーブル
９　送信元ＶＰＮ識別テーブル
１０　パケット受信部
１１　パケット中継部
１２　パケット送信部
１４　送信インタフェース
５１　パケット中継手段
５２　ネットワーク間中継手段
５３　ドメイン間中継手段
５４　経路情報管理手段
１００　中継装置

【書類名】　　図面

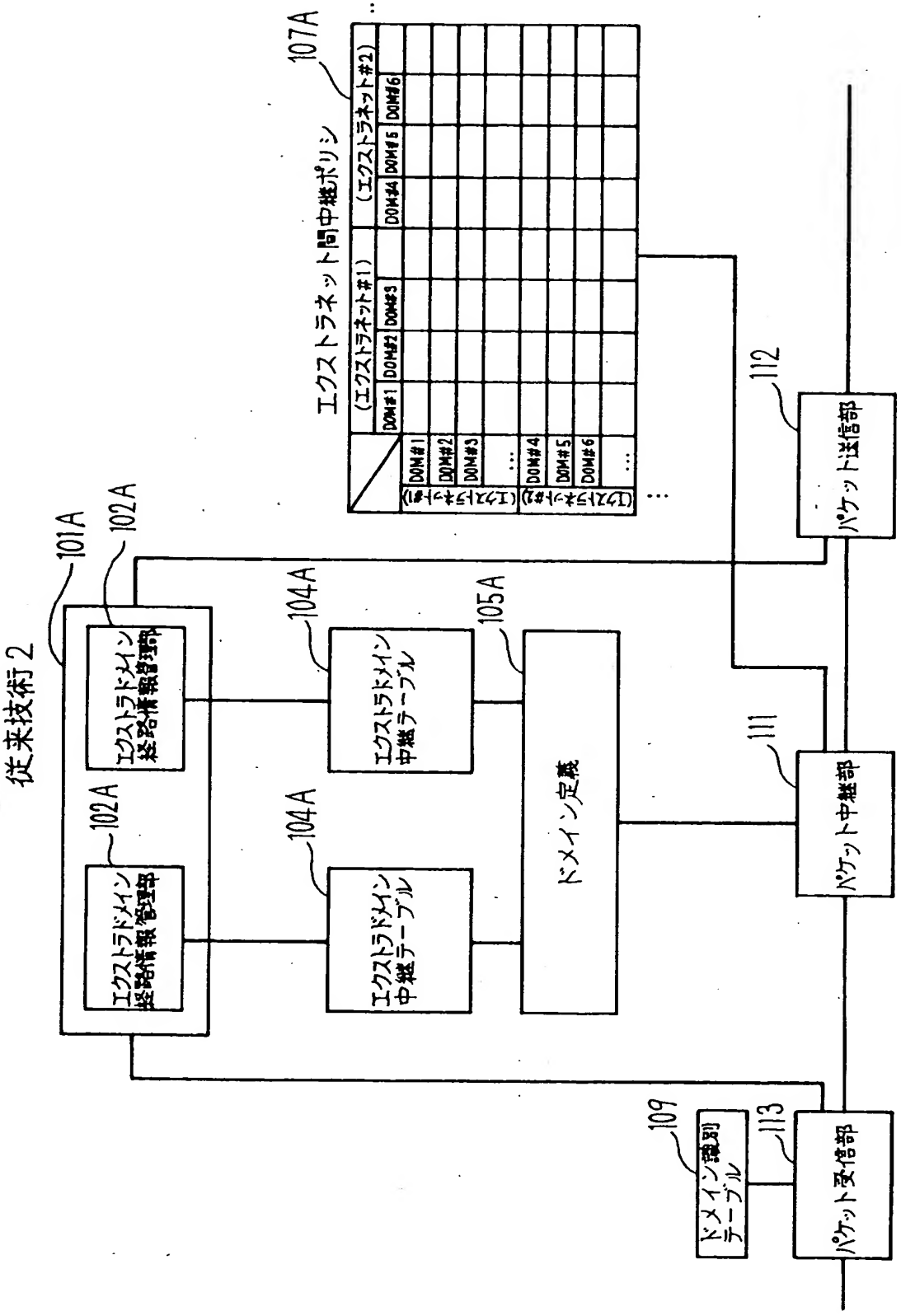
【図１】


ＶＰＮの運用形態
イントラネット
エクストラネット
シングル経路ドメイン
マルチ経路ドメイン
経路ドメイン＃1
拠点1 管理主体＝A
拠点2 管理主体＝A
拠点3 管理主体＝A
イントラネット
経路ドメイン＃2
経路ドメイン＃3
拠点1 管理主体＝A
拠点2 管理主体＝B
拠点3 管理主体＝C
エクストラネット

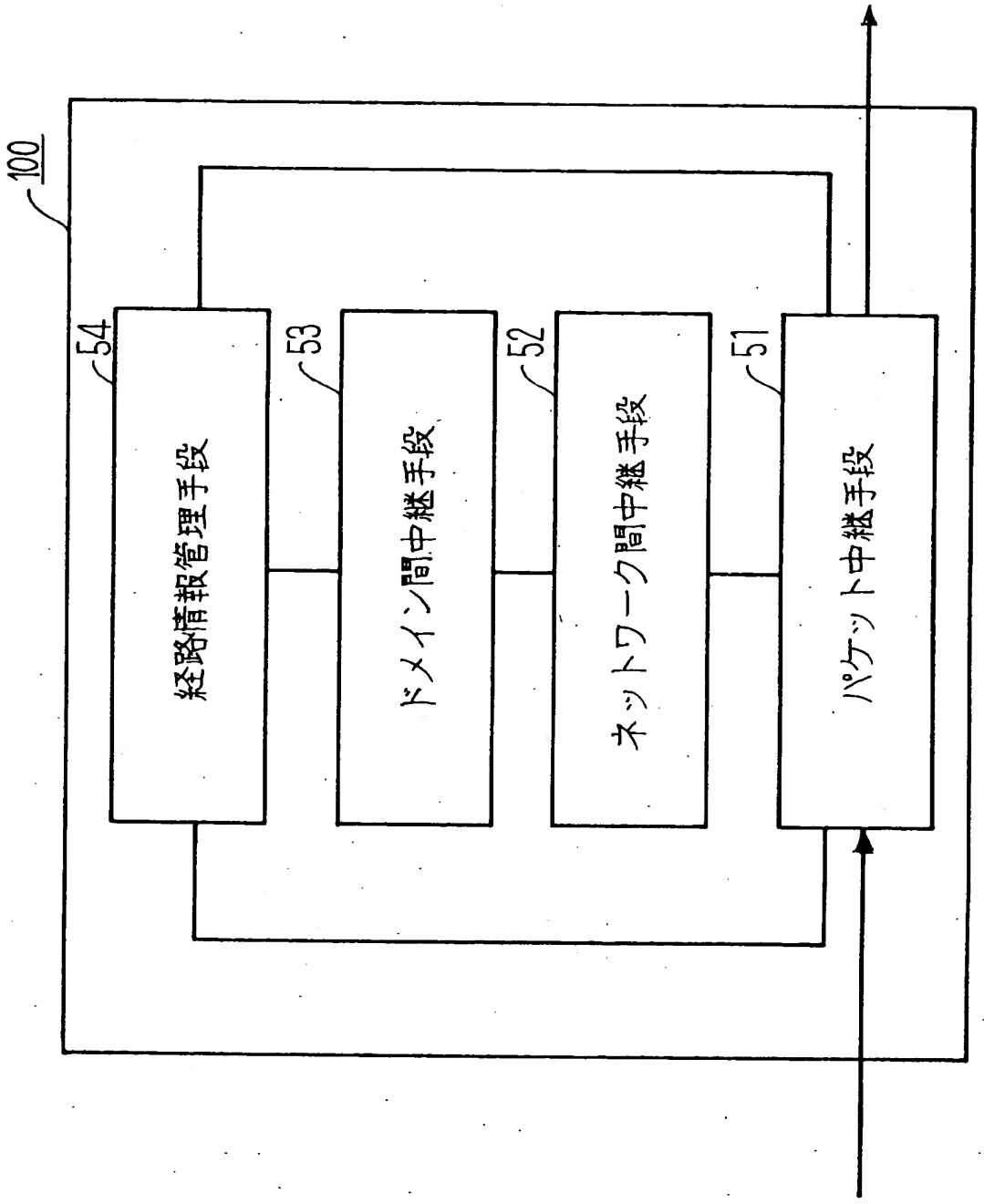
【図２】


（従来技術）エクストラネットを代表するドメインに対する中継テーブルにそれぞれ重複する経路を書き込む方法
101
ドメイン#12
102
イントラネットドメイン経路情報管理部
ドメイン#11
102
イントラネットドメイン経路情報管理部
104
ドメイン#12
イントラネットドメイン中継テーブル
104
ドメイン#11
イントラネットドメイン中継テーブル
111
パケット中継部
112
パケット送信部
109
ドメイン識別テーブル
113
パケット受信部

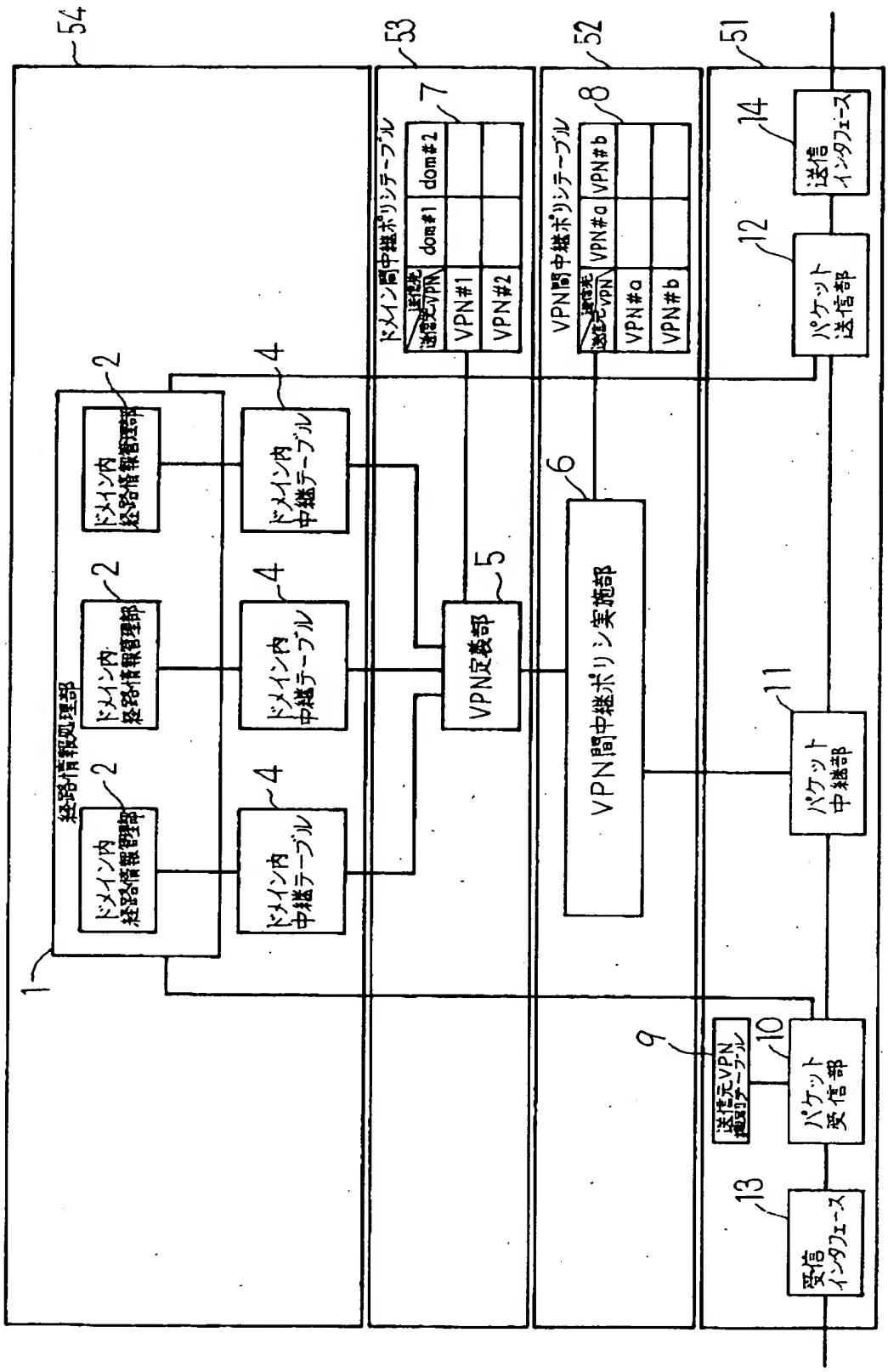
【図３】


従来技術２
101A
102A
エクストラドメイン経路情報管理部
102A
エクストラドメイン経路情報管理部
104A
エクストラドメイン中継テーブル
104A
エクストラドメイン中継テーブル
105A
ドメイン定義
107A
エクストラネット間中継ポリシ
(エクストラネット#1)
(エクストラネット#2)
DOM#1
DOM#2
DOM#3
DOM#4
DOM#5
DOM#6
111
パケット中継部
112
パケット送信部
113
パケット受信部
109
ドメイン識別テーブル

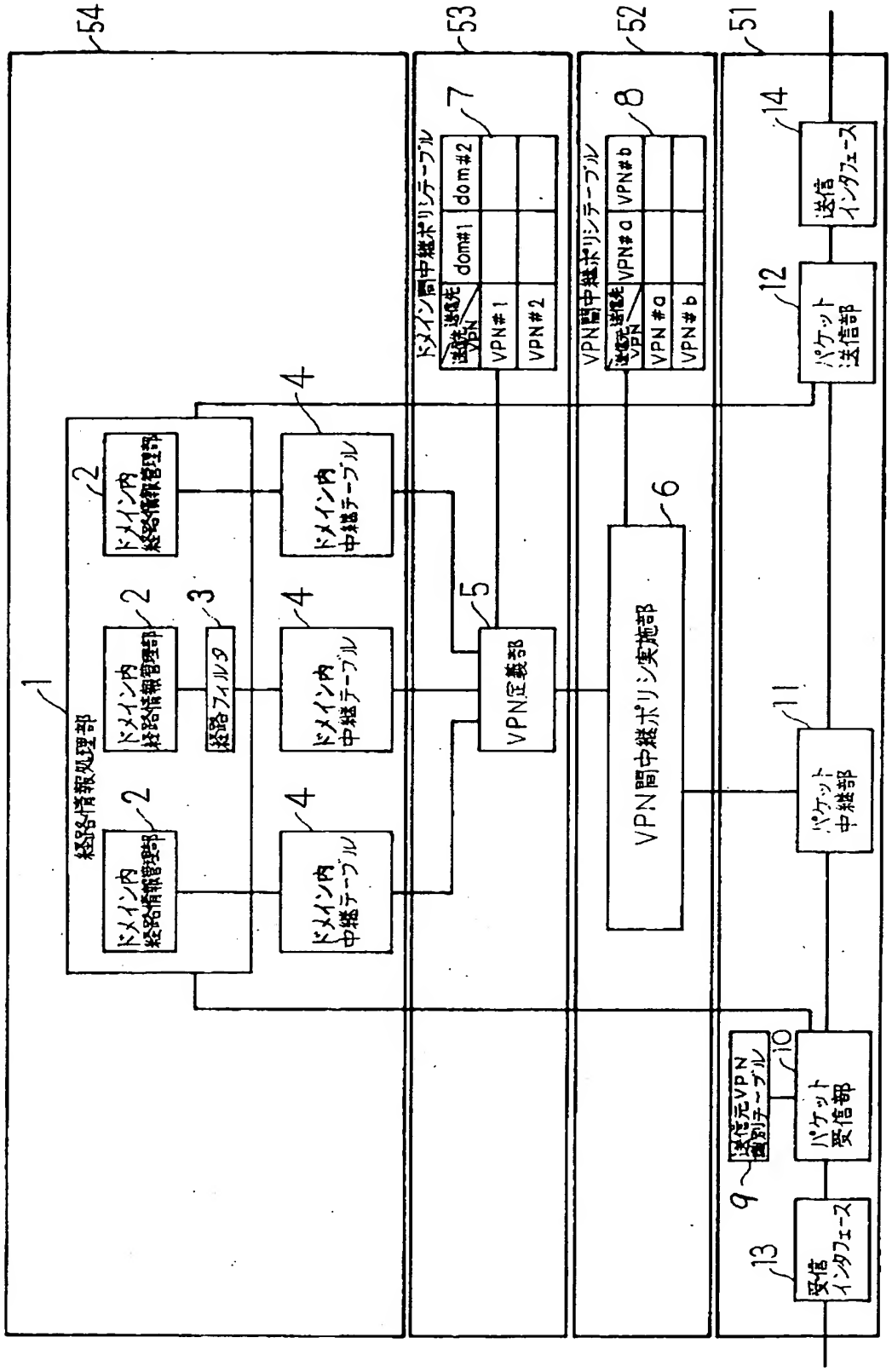
【図４】



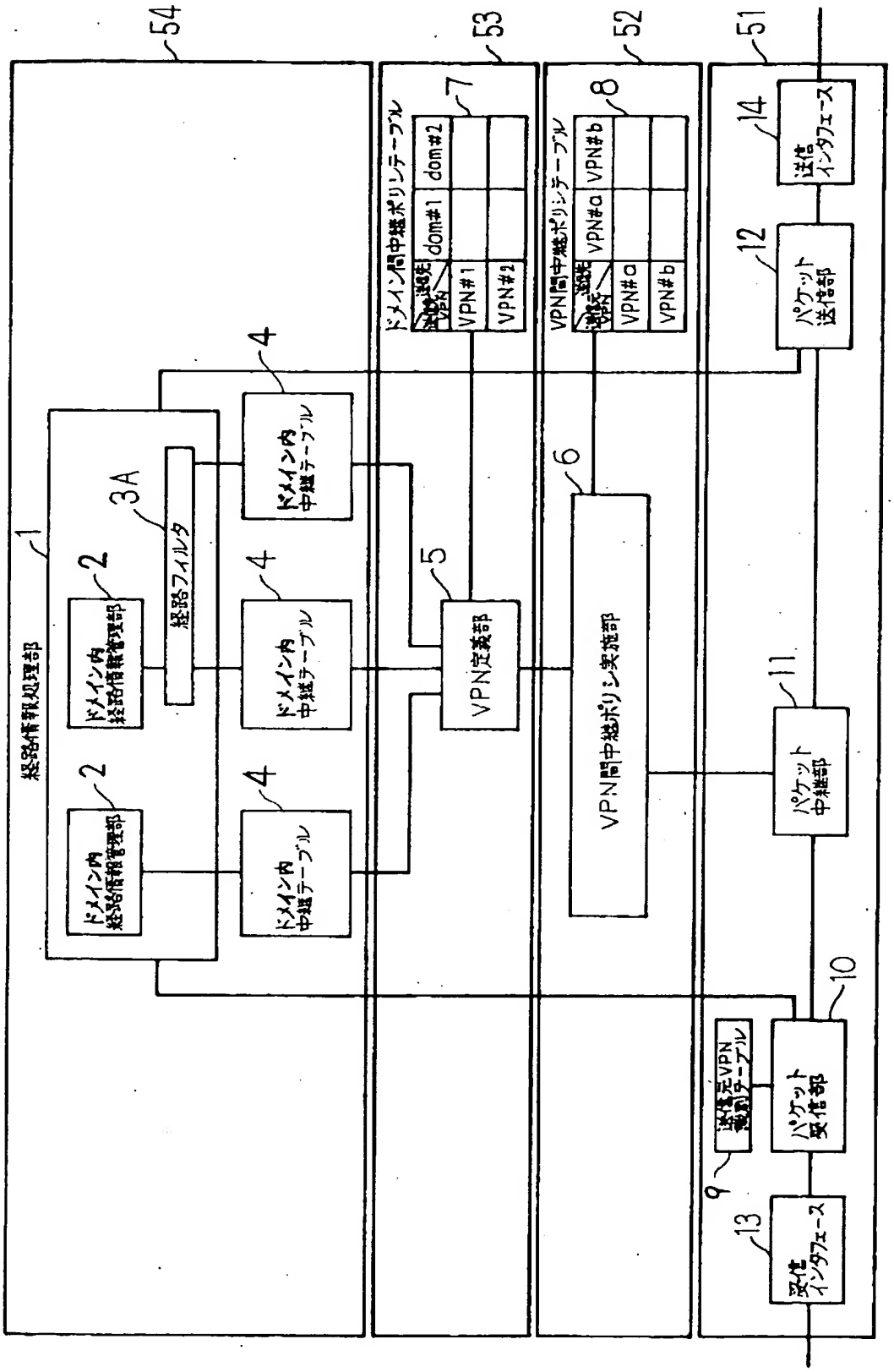
【図５】


54
53
52
51
経路情報処理部
1
ドメイン内経路情報管理部
2
ドメイン内中継テーブル
4
VPN定義部
5
VPN間中継ポリシ実施部
6
ドメイン間中継ポリシテーブル
7
VPN間中継ポリシテーブル
8
送信元VPN
dom#1
dom#2
VPN#1
VPN#2
VPN#a
VPN#b
送信元VPNテーブル
9
パケット受信部
10
パケット中継部
11
パケット送信部
12
受信インタフェース
13
送信インタフェース
14

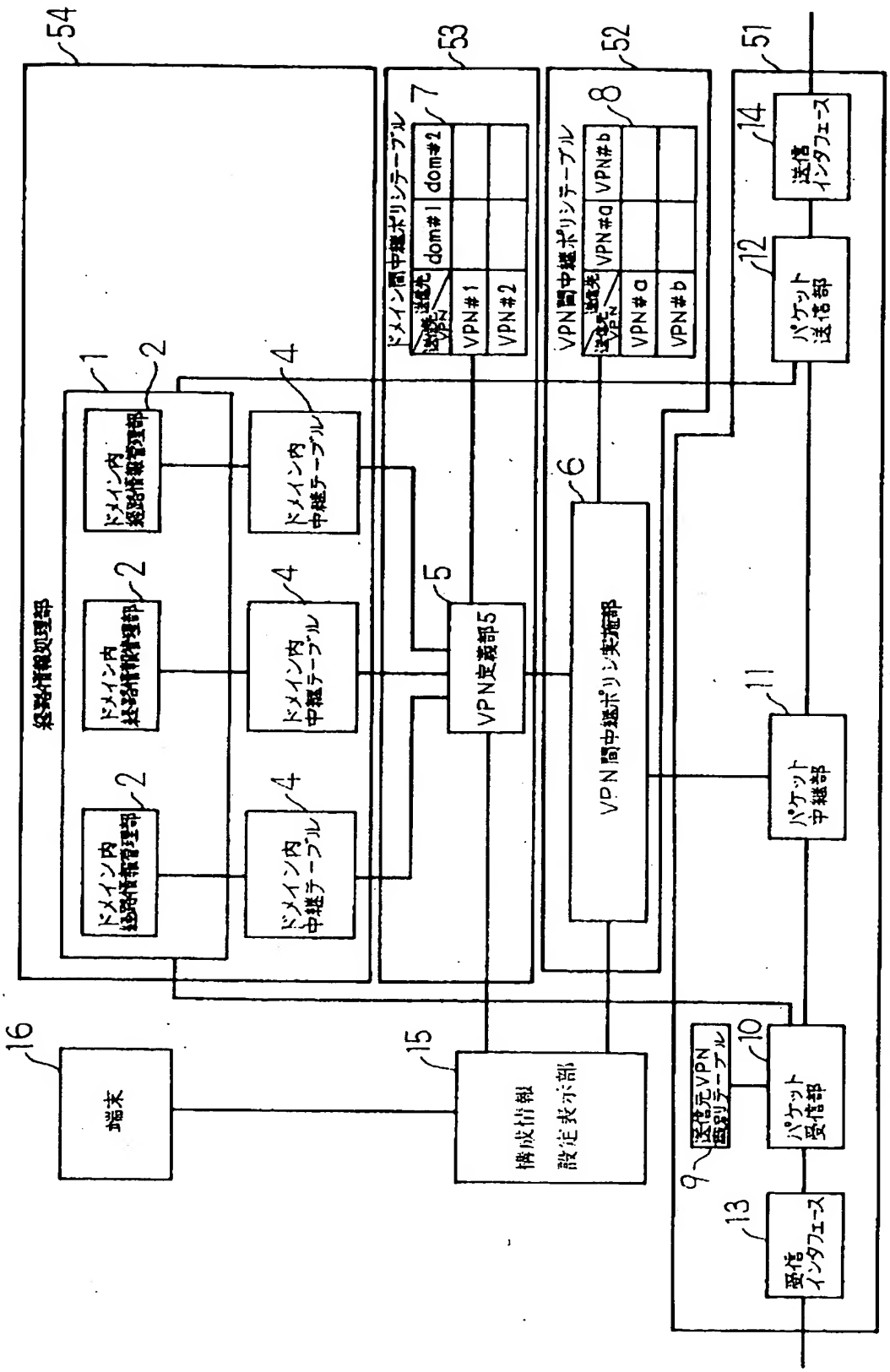
【図６】


54
53
52
51
1
経路情報処理部
2
ドメイン内経路情報管理部
3
経路フィルタ
4
ドメイン内中継テーブル
5
VPN定義部
6
VPN間中継ポリシ実施部
7
ドメイン間中継ポリシテーブル
送信元VPN
送信先VPN
dom#1
dom#2
VPN#1
VPN#2
8
VPN間中継ポリシテーブル
VPN#a
VPN#b
9
送信元VPN識別テーブル
10
パケット受信部
11
パケット中継部
12
パケット送信部
13
受信インタフェース
14
送信インタフェース

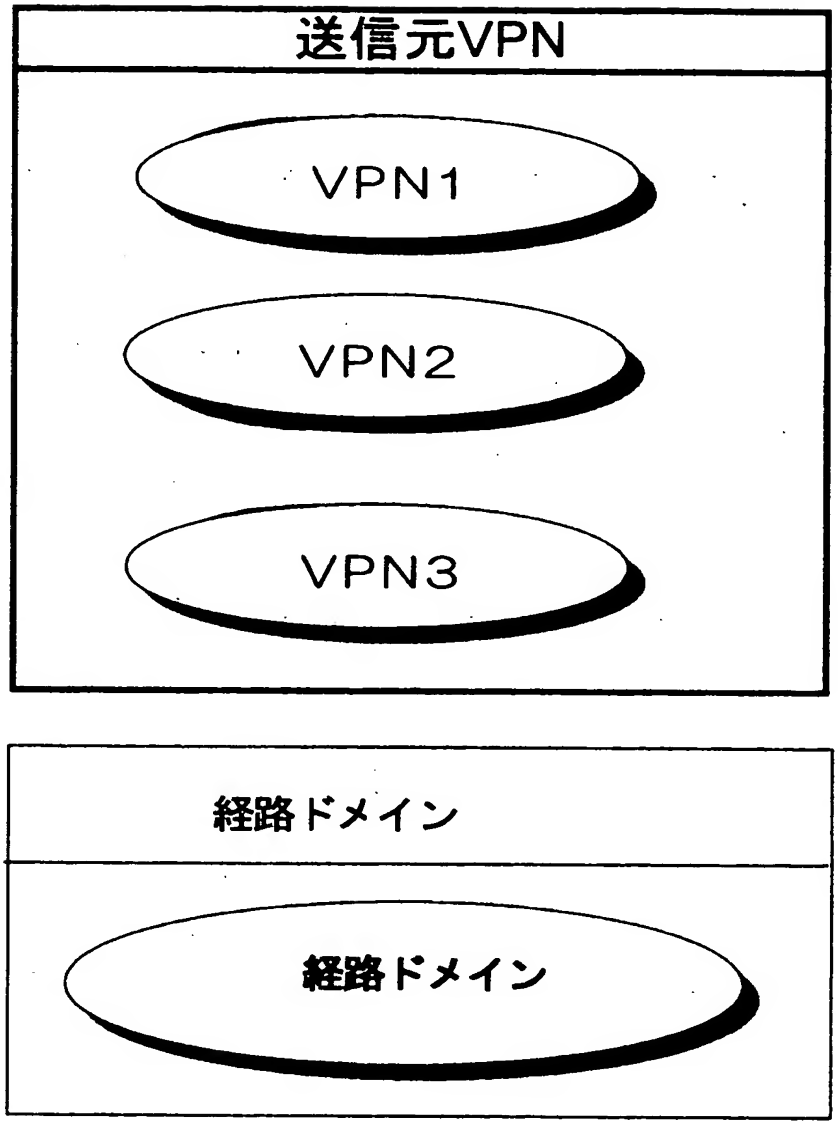
【図７】


経路情報処理部
1
ドメイン内経路情報管理部
2
ドメイン内経路情報管理部
2
経路フィルタ
3A
ドメイン内中継テーブル
4
ドメイン内中継テーブル
4
ドメイン内中継テーブル
4
VPN定義部
5
VPN間中継ポリシ実施部
6
ドメイン間中継ポリシテーブル
7
VPN間中継ポリシテーブル
8
パケット中継部
11
パケット送信部
12
送信インタフェース
14
パケット受信部
10
送信元VPN識別テーブル
9
受信インタフェース
13
54
53
52
51

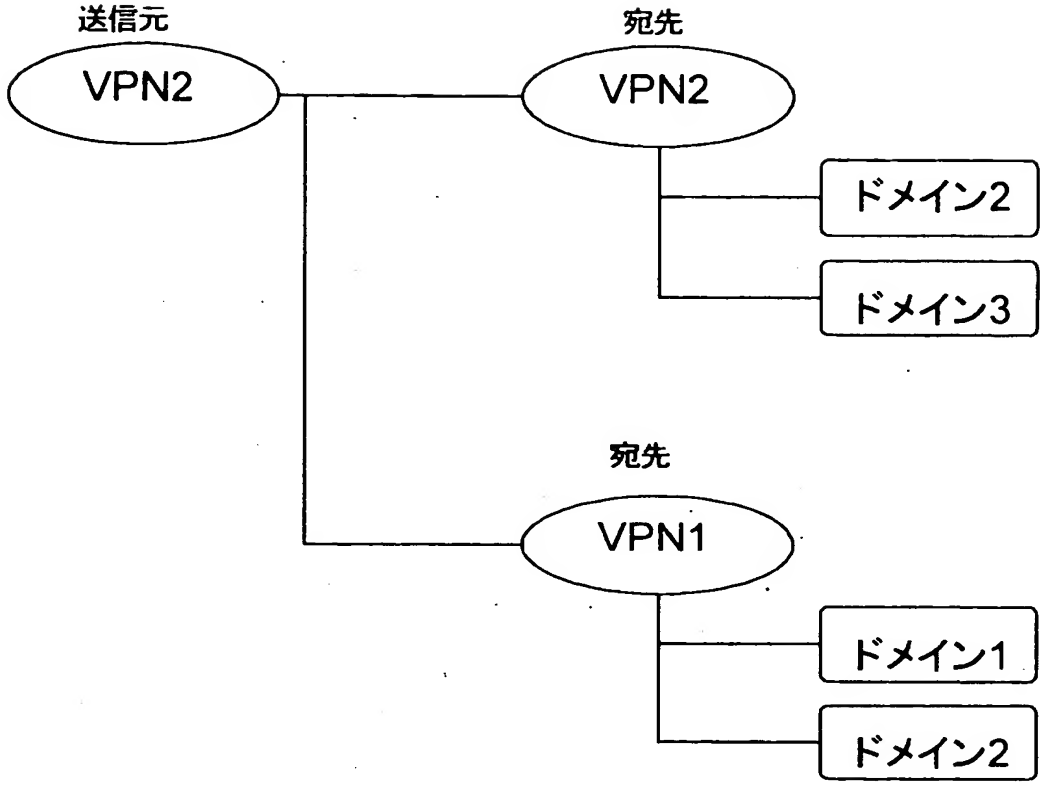
【図８】


54
53
52
51
1
2
4
5
6
7
8
9
10
11
12
13
14
15
16
経路情報処理部
ドメイン内経路情報管理部
ドメイン内中継テーブル
VPN定義部5
VPN間中継ポリシ実施部
ドメイン間中継ポリシテーブル
VPN間中継ポリシテーブル
送信元VPN識別テーブル
パケット中継部
パケット送信部
パケット受信部
送信インタフェース
受信インタフェース
構成情報設定表示部
端末
dom#1
dom#2
VPN#1
VPN#2
VPN#a
VPN#b

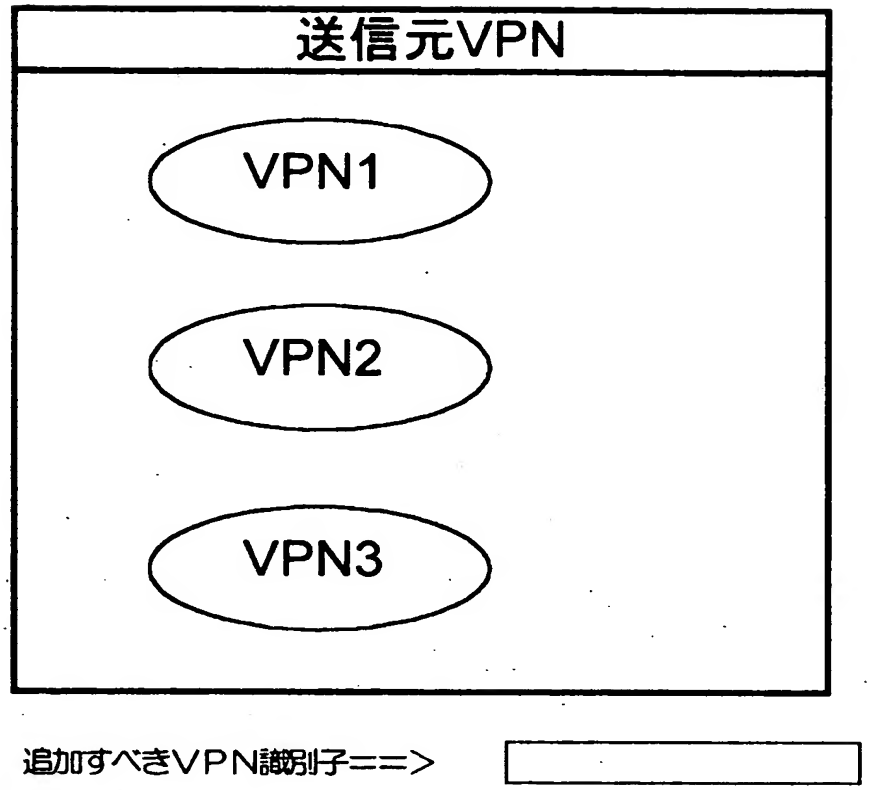
【図９】



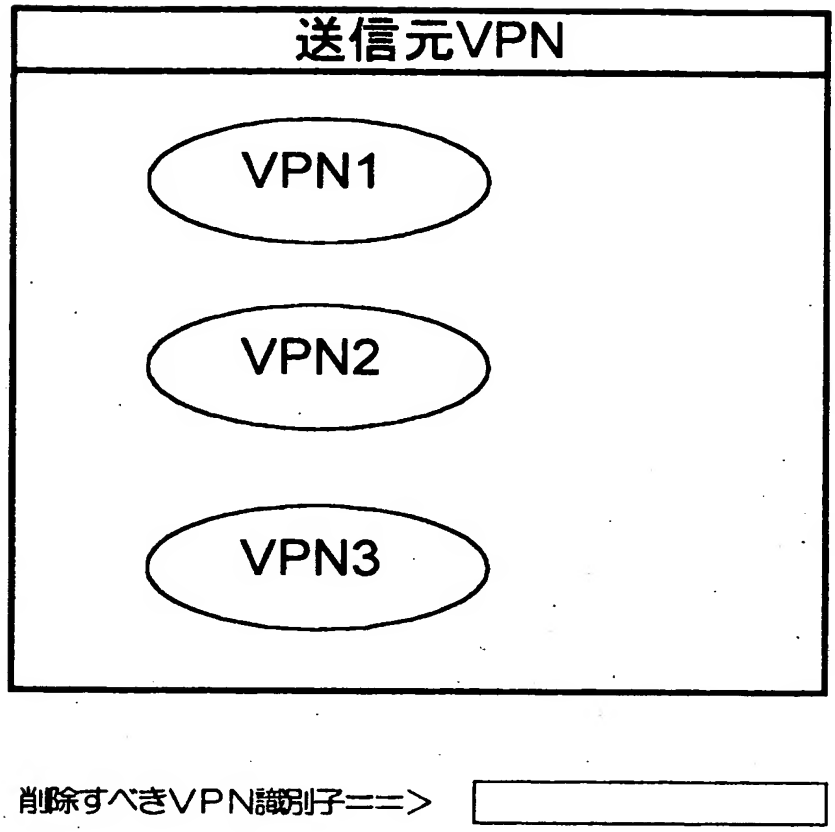
【図１０】



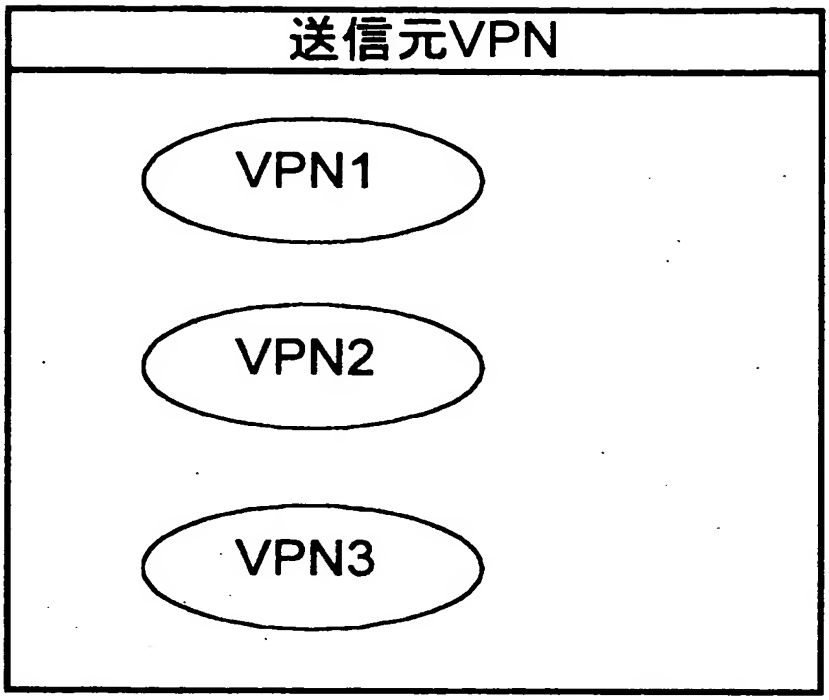
【図１１】



【図１２】

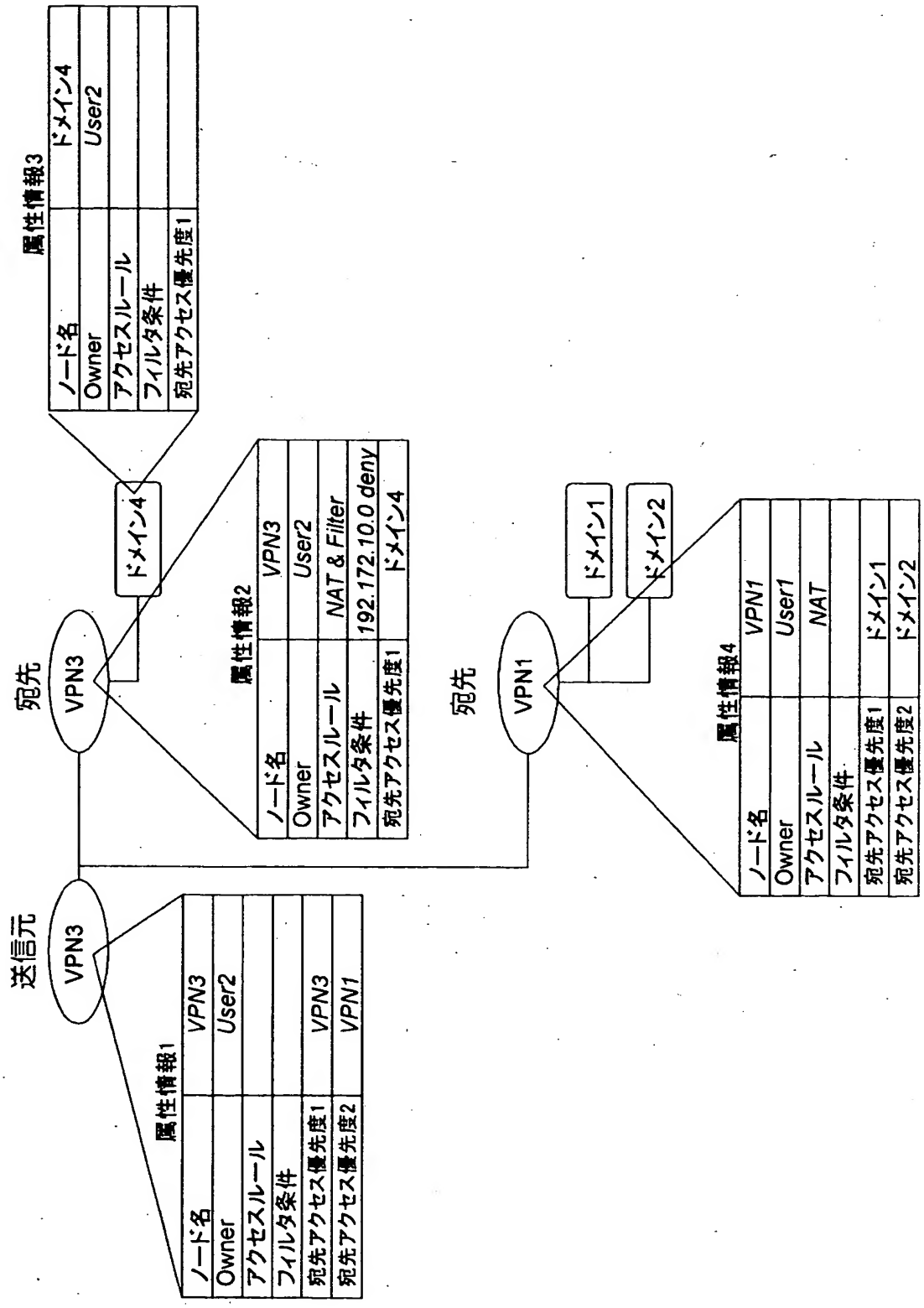


【図１３】

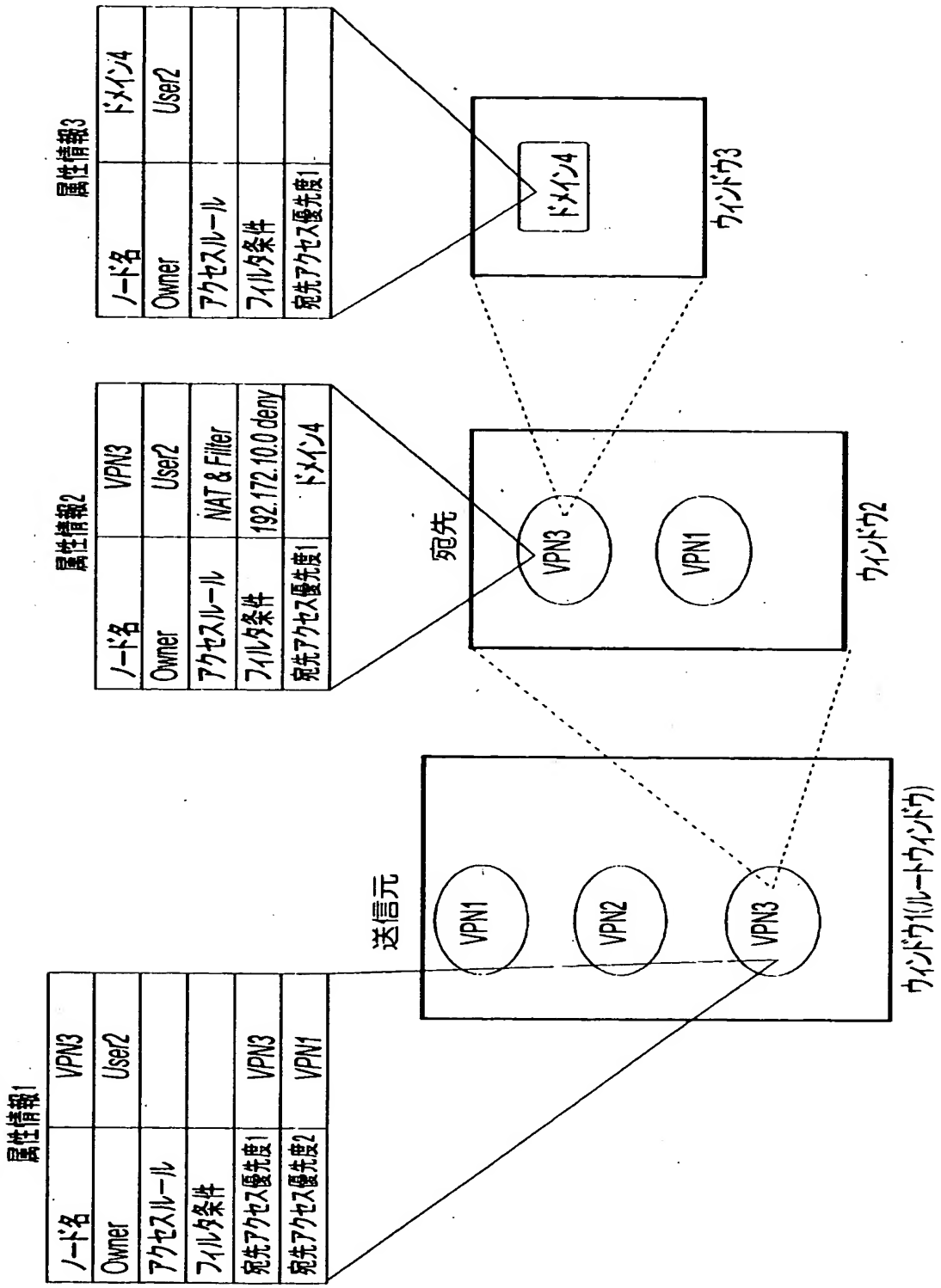



名称を変更すべきＶＰＮ識別子==>

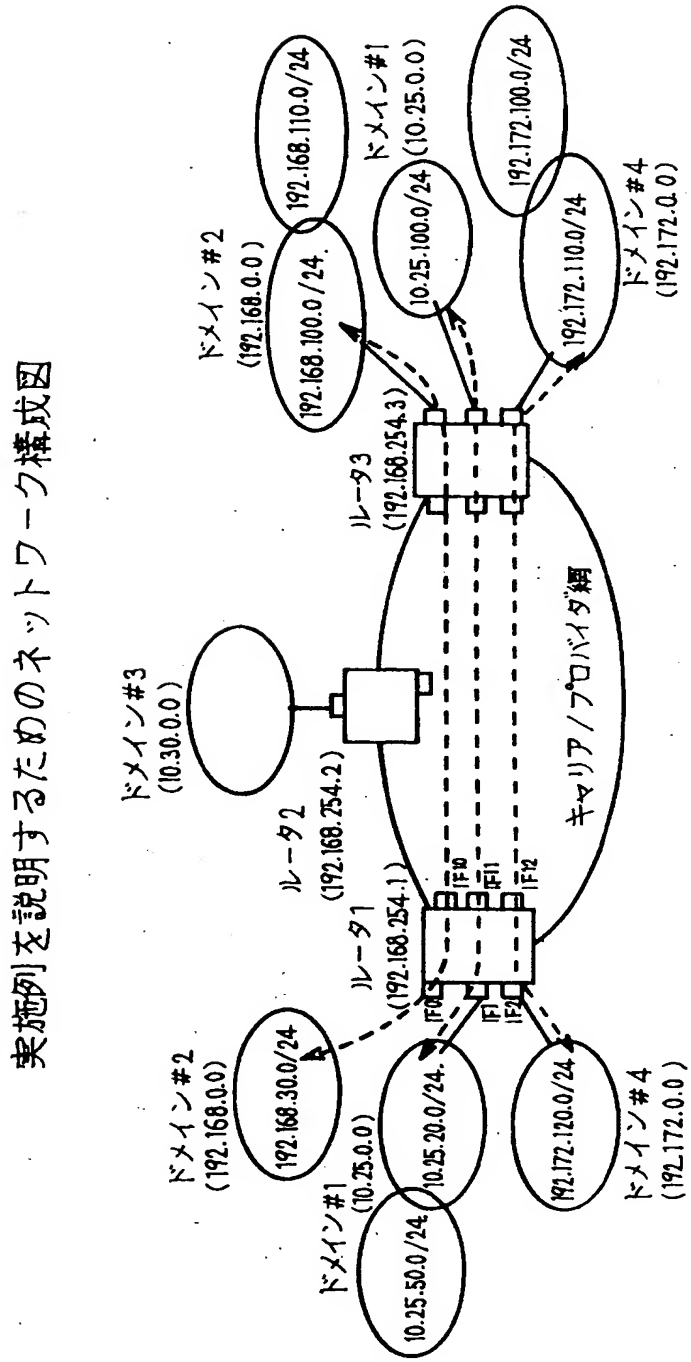
【図１４】


送信元
VPN3
宛先
VPN3
宛先
VPN1
ドメイン4
ドメイン1
ドメイン2
属性情報1
ノード名 VPN3
Owner User2
アクセスルール
フィルタ条件
宛先アクセス優先度1 VPN3
宛先アクセス優先度2 VPN1
属性情報2
ノード名 VPN3
Owner User2
アクセスルール NAT & Filter
フィルタ条件 192.172.10.0 deny
宛先アクセス優先度1 ドメイン4
属性情報3
ノード名 ドメイン4
Owner User2
アクセスルール
フィルタ条件
宛先アクセス優先度1
属性情報4
ノード名 VPN1
Owner User1
アクセスルール NAT
フィルタ条件
宛先アクセス優先度1 ドメイン1
宛先アクセス優先度2 ドメイン2

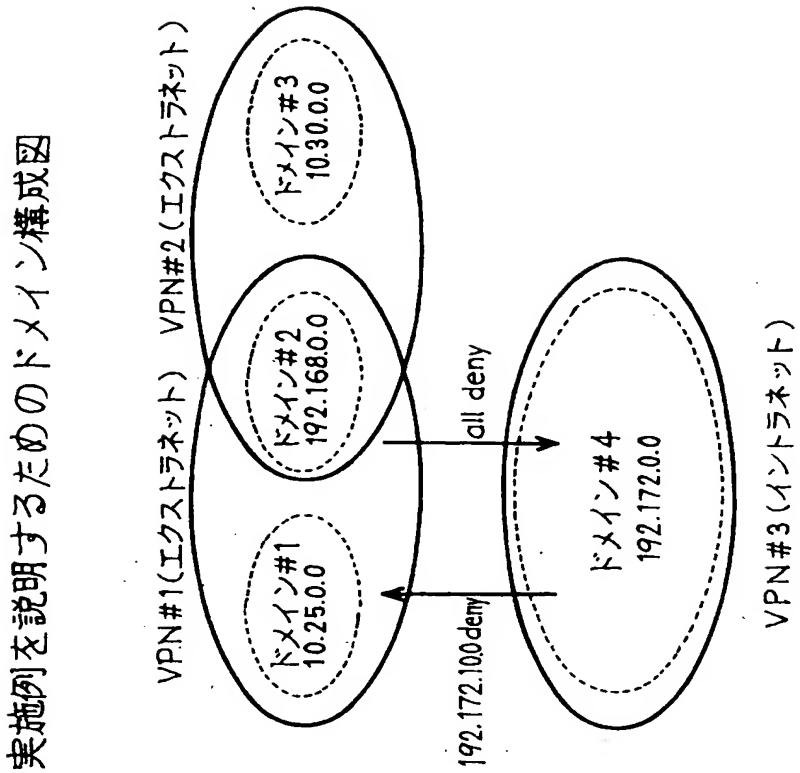
【図１５】


属性情報1
ノード名
VPN3
Owner
User2
アクセスルール
フィルタ条件
宛先アクセス優先度1
VPN3
宛先アクセス優先度2
VPN1
送信元
VPN1
VPN2
VPN3
ウィンドウ1(ルートウィンドウ)
属性情報2
ノード名
VPN3
Owner
User2
アクセスルール
NAT & Filter
フィルタ条件
192.172.10.0 deny
宛先アクセス優先度1
ドメイン4
宛先
VPN3
VPN1
ウィンドウ2
属性情報3
ノード名
ドメイン4
Owner
User2
アクセスルール
フィルタ条件
宛先アクセス優先度1
ドメイン4
ウィンドウ3

【図１６】


実施例を説明するためのネットワーク構成図
ドメイン#2
(192.168.0.0)
192.168.110.0/24
192.168.100.0/24
ドメイン#1
(10.25.0.0)
10.25.100.0/24
192.172.100.0/24
ドメイン#4
(192.172.0.0)
192.172.110.0/24
ルータ3
(192.168.254.3)
キャリア/プロバイダ網
ドメイン#3
(10.30.0.0)
ルータ2
(192.168.254.2)
IF10
IF11
IF12
ルータ1
(192.168.254.1)
IF0
IF1
IF2
ドメイン#2
(192.168.0.0)
192.168.30.0/24
ドメイン#1
(10.25.0.0)
10.25.20.0/24
10.25.50.0/24
192.172.120.0/24
ドメイン#4
(192.172.0.0)

【図１７】


実施例を説明するためのドメイン構成図
VPN#1(エクストラネット)
VPN#2(エクストラネット)
ドメイン#1
10.25.0.0
ドメイン#2
192.168.0.0
ドメイン#3
10.30.0.0
all deny
192.172.10.0deny
ドメイン#4
192.172.0.0
VPN#3(イントラネット)

【図１８】

| 受信インタフェース | 送信元ドメイン | 送信元ＶＰＮ |
|---|---|---|
| IF#0 | ドメイン#2 | VPN#1 |
| IF#1 | ドメイン#1 | VPN#1 |
| IF#2 | ドメイン#4 | VPN#3 |

【図１９】

VPN間中継ポリシテーブル

| 参照順位 / 受信ドメイン | 1 位 | 2 位 |
|---|---|---|
| VPN#1 | VPN#1 permit | |
| VPN#2 | VPN#2 permit | VPN#1 permit |
| VPN#3 | VPN#3 permit | VPN#1 192.172.10.0 deny |

【図２０】

ドメイン間中継ポリシテーブル

| 参照順位 / 受信 | 1位 | 2位 | … |
|---|---|---|---|
| VPN#1 | ドメイン#1 permit | ドメイン#2 permit | |
| VPN#2 | ドメイン#2 permit | ドメイン#3 permit | |
| VPN#3 | ドメイン#4 permit | | |

【図２１】

ドメイン内中継テーブル（ドメイン＃１）

| Destination | mask | 出力インタフェース | 次ホップルータ |
|---|---|---|---|
| 10.25.20.0 | 255.255.255.0 | IF1 | 10.25.20.1 |
| 10.25.50.0 | 255.255.255.0 | IF1 | 10.25.50.1 |
| 10.25.100.0 | 255.255.255.0 | IF11 | 192.168.254.3 |

【図２２】

ドメイン内中継テーブル（ドメイン＃２）

| Destination | mask | 出力インタフェース | 次ホップルータ |
|---|---|---|---|
| 192.168.30.0 | 255.255.255.0 | IF0 | 192.168.30.0 |
| 192.168.100.0 | 255.255.255.0 | IF10 | 192.168.254.3 |
| 192.168.110.0 | 255.255.255.0 | IF10 | 192.168.254.3 |

【図２３】

ドメイン内中継テーブル（ドメイン＃４）

| Destination | mask | 出力インタフェース | 次ホップルータ |
|---|---|---|---|
| 192.172.100.0 | 255.255.255.0 | IF12 | 192.168.254.3 |
| 192.172.110.0 | 255.255.255.0 | IF12 | 192.168.254.3 |
| 192.172.120.0 | 255.255.255.0 | IF2 | 192.172.120.1 |

【書類名】　要約書

【要約】

【目的】　本発明は、パケット中継装置における中継ポリシの設定／変更を容易にすること、また、パケット中継装置で使用されるメモリの使用量の削減することを目的とする。

【構成】　中継装置１００において、入力されたパケットに対応する送信元ネットワーク識別子に基づき、該パケットの中継が許されている１つ以上のネットワークを選択するネットワーク間中継手段５２と、前記１つ以上のネットワークに対応する１つ以上の経路ドメインを選択するドメイン間中継手段５３と、前記パケットの送信先アドレスと前記１つ以上の経路ドメインの各経路ドメイン情報とを照合して前記パケットを次のパケット中継装置に送出するための次ポップルータアドレスを選択する経路情報管理手段５４と、前記送出先アドレスに前記パケットを送出するパケット中継手段５１とを有するように構成する。

【選択図】　図4



出証特２００１－３０８０８８２

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社